

Source: TSG CT WG1
Title: CRs on Rel-5 WI “IMS-CCR” for TSs 24.229 and 24.228
Agenda item: 7.17
Document for: APPROVAL

This document contains 17 **CRs for Rel-5 WI “IMS-CCR”** (including mirror CRs), that have been agreed by TSG CT WG1 meeting #38 and forwarded to TSG CT Plenary meeting #28 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Ver	WI	Rel
C1-050521	Correction Reg-Await-Auth Timer	24.229	878		F	5.12.0	IMS-CCR	Rel-5
C1-050522	Correction Reg-Await-Auth Timer	24.229	879		A	6.6.0	IMS-CCR	Rel-6
C1-050523	Security Association In P-CSCF	24.229	880		F	5.12.0	IMS-CCR	Rel-5
C1-050524	Security Association in P-CSCF	24.229	881		A	6.6.0	IMS-CCR	Rel-6
C1-050658	SDP representation of AMR	24.228	138	1	F	5.12.0	IMS-CCR	Rel-5
C1-050673	Port 5060	24.229	869	1	F	5.12.0	IMS-CCR	Rel-5
C1-050674	Port 5060	24.229	871	1	A	6.6.0	IMS-CCR	Rel-6
C1-050685	Call-Id mismatch in the protected REGISTER when reg-await-auth timer is running	24.229	917	1	F	5.12.0	IMS-CCR	Rel-5
C1-050688	Correction of error in the specification of the extension to Authorization header	24.229	920	1	F	5.12.0	IMS-CCR	Rel-5
C1-050689	Correction of error in the specification of the extension to Authorization header	24.229	921	1	A	6.6.0	IMS-CCR	Rel-6
C1-050776	SIP headers storage for P-CSCF initiated session release	24.229	922		F	5.12.0	IMS-CCR	Rel-5
C1-050777	SIP headers storage for P-CSCF initiated session release	24.229	891	2	A	6.6.0	IMS-CCR	Rel-6
C1-050780	S-CSCF failure	24.229	859	2	F	5.12.0	IMS-CCR	Rel-5
C1-050782	Handling of P-Associated URI header	24.229	885	2	F	5.12.0	IMS-CCR	Rel-5
C1-050783	Handling of P-Associated URI header	24.229	886	2	A	6.6.0	IMS-CCR	Rel-6
C1-050784	Clarification to the procedures at the I-CSCF	24.229	906	2	F	5.12.0	IMS-CCR	Rel-5
C1-050785	Clarification to the procedures at the I-CSCF	24.229	907	2	A	6.6.0	IMS-CCR	Rel-6

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 878** ⌘ rev **-** ⌘ Current version: **5.c.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Correction Reg-Await-Auth Timer		
Source:	⌘ Siemens		
Work item code:	⌘ IMS-CCR	Date:	⌘ 05/04/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ Current description in clause 7.8 implies that the P-CSCF implements the reg-await-auth timer. However, this timer is only implemented in the S-CSCF
Summary of change:	⌘ P-CSCF use the value of the reg-await-auth timer to set the timer of the temporary SIP level lifetimer of a security association. Description in clause 7.8 is aligned with description in subclause 5.2
Consequences if not approved:	⌘ Handling of security association not possible

Clauses affected:	⌘ 7.8						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘			
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘			
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
Other comments:	⌘						

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7.8 IM CN subsystem timers

Table 7.9 shows recommended values for timers specific to the IM CN subsystem.

Table 7.9: IM CN subsystem

Timer	Value to be applied at the UE	Value to be applied at the P-CSCF	Value to be applied at the S-CSCF	Meaning
reg-await-auth	Not applicable	4 minutes Not applicable	4 minutes	<p>The timer is used by the S-CSCF during the authentication procedure of the UE. For detailed usage of the timer see subclause 5.4.1.2.</p> <p>The timer is also used by the P-CSCF to set the SIP level lifetime of the temporary set of security associations. For detailed usage of the timer see subclause 5.1.1.5.</p> <p>The authentication procedure may take in the worst case as long as 2 times Timer F. The IM CN subsystem value for Timer F is 128 seconds.</p>

Note: [The UE and the P-CSCF use the value of the reg-await-auth timer to set the SIP level lifetime of the temporary set of security associations.](#)

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 879** ⌘ rev **-** ⌘ Current version: **6.6.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Correction Reg-Await-Auth Timer		
Source:	⌘ Siemens		
Work item code:	⌘ IMS-CCR	Date:	⌘ 04/04/2005
Category:	⌘ A	Release:	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ Current description in clause 7.8 implies that the P-CSCF implements the reg-await-auth timer. However, this timer is only implemented in the S-CSCF.
Summary of change:	⌘ P-CSCF use the value of the reg-await-auth timer to set the timer of the temporary SIP level lifetimer of a security association. Description in clause 7.8 is aligned with description in subclause 5.2
Consequences if not approved:	⌘ Handling of security association not possible.

Clauses affected:	⌘ 7.8						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘			
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘			
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
Other comments:	⌘						

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*** 1st change ***

7.8 IM CN subsystem timers

Table 7.9 shows recommended values for timers specific to the IM CN subsystem.

Table 7.9: IM CN subsystem

Timer	Value to be applied at the UE	Value to be applied at the P-CSCF	Value to be applied at the S-CSCF	Meaning
reg-await-auth	not applicable	4 minutes not applicable	4 minutes	<p>The timer is used by the S-CSCF during the authentication procedure of the UE. For detailed usage of the timer see subclause 5.4.1.2.</p> <p>The timer is also used by the P-CSCF to set the SIP level lifetime of the temporary set of security associations. For detailed usage of the timer see subclause 5.1.1.5.</p> <p>The authentication procedure may take in the worst case as long as 2 times Timer F. The IM CN subsystem value for Timer F is 128 seconds.</p>

Note: The UE and the P-CSCF use the value of the reg-await-auth timer to set the SIP level lifetime of the temporary set of security associations.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 880** ⌘ rev **-** ⌘ Current version: **5.c.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Security Association in P-CSCF		
Source:	⌘ Siemens		
Work item code:	⌘ IMS-CCR	Date:	⌘ 05/04/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ Current description of handling of security association in P-CSCF does not cover the case where the UE sends a reREGISTER using an existing security association
Summary of change:	⌘ On reception of 200 OK and an already existing set of security association is available in the P-CSCF, then the lifetime of the security association has to be set to the longest of either the existing lifetime of the lifetime of the just completed registration plus 30 seconds. This procedure is inline with the one in the UE
Consequences if not approved:	⌘ Security Association time out in P-CSCF even in case the UE has reregistered

Clauses affected:	⌘ 5.2.2										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications Test specifications O&M Specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
Other comments:	⌘										

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

- 1) insert a Path header in the request including an entry containing:
 - the SIP URI identifying the P-CSCF;
 - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;
- 2) insert a Require header containing the option tag "path";
- 3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];
- 4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";
- 5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;
- 6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:
 - a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
 - b) if the security association the REGISTER request was received on, is an already established one, then:
 - the P-CSCF shall remove the Security-Verify header if it is present, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
 - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
 - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and
 - c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;
- 7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;
- 3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;
- 2) associate the Service-Route header list with the registered public user identity;
- 3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

- 5) store the values received in the P-Charging-Function-Addresses header;

6) if an existing set of security association is available, set the SIP level lifetime of the security association to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds;

67) if a set of temporary security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

78) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

- 1) reduce the SIP level lifetime of the old set of security associations towards the same UE to $64 \cdot T1$ (if currently longer than $64 \cdot T1$); and

- 2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 3: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 4: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than $64 * T1$ and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly established set of security associations for further messages towards the UE as appropriate (see NOTE 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

- 1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;
- 2) keep the newly established set of security associations created during this authentication;
- 3) delete, if existing, any other set of security associations towards this UE immediately; and,
- 4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) response for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

- 1) keep the newly established set of security associations created during this authentication;
- 2) delete, if existing, any other set of security associations towards this UE immediately; and,
- 3) use the kept newly established set of security associations for further messages sent towards the UE.

NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2-1.

Table 5.2.2-1: Handling of security associations at the P-CSCF

	Temporary set of security associations	Newly established set of security associations	Old set of security associations
SIP message received over newly established set of security associations that have not yet been taken into use	No action	Take into use	Reduce SIP level lifetime to $64 \cdot T1$, if lifetime is larger than $64 \cdot T1$
SIP message received over old set of security associations	No action	No action	No action
Old set of security associations currently in use will expire in $64 \cdot T1$	No action	Take into use	No action
Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request	Create Remove any previously existing temporary set of security associations	No action	No action
Sending 200 (OK) response for REGISTER request that concludes re-authentication	Change to a newly established set of security associations	Convert to and treat as old set of security associations (see next column)	Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received. Delete all other old sets of security associations immediately
Sending 200 (OK) response for REGISTER request that concludes initial authentication	Change to a newly established set of security associations and take into use immediately	Convert to old set of security associations, i.e. delete	Delete

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 881** ⌘ rev **-** ⌘ Current version: **6.6.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Security Association in P-CSCF		
Source:	⌘ Siemens		
Work item code:	⌘ IMS-CCR	Date:	⌘ 05/04/2005
Category:	⌘ A	Release:	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ Current description of handling of security association in P-CSCF does not cover the case where the UE sends a reREGISTER using an existing security association.
Summary of change:	⌘ On reception of 200 OK and an already existing set of security association is available in the P-CSCF, then the lifetime of the security association has to be set to the longest of either the existing lifetime of the lifetime of the just completed registration plus 30 seconds. This procedure is inline with the one in the UE.
Consequences if not approved:	⌘ Security Association time out in P-CSCF even in case the UE has reregistered

Clauses affected:	⌘ 5.2.2										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications Test specifications O&M Specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
Other comments:	⌘										

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

- 1) insert a Path header in the request including an entry containing:
 - the SIP URI identifying the P-CSCF;
 - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;
- 2) insert a Require header containing the option tag "path";
- 3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];
- 4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";
- 5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. If the header is not present, then the P-CSCF shall return a suitable 4xx response;
- 6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:
 - a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header;
 - b) if the security association the REGISTER request was received on, is an already established one, then:
 - the P-CSCF shall remove the Security-Verify header if it is present;
 - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
 - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and
 - c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;
- 7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;

- 2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;
- 3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;
- 2) associate the Service-Route header list with the registered public user identity;
- 3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

- 5) store the values received in the P-Charging-Function-Addresses header;

6) if an existing set of security association is available, set the SIP level lifetime of the security association to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds;

7) if a temporary set of security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

8) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

- 1) reduce the SIP level lifetime of the old set of security associations towards the same UE to 64*T1 (if currently longer than 64*T1); and
- 2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 3: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 4: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than $64 * T1$ and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly established set of security associations for further messages towards the UE as appropriate (see NOTE 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

- 1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;
- 2) keep the newly established set of security associations created during this authentication;
- 3) delete, if existing, any other set of security associations towards this UE immediately; and
- 4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) response for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

- 1) keep the newly established set of security associations created during this authentication;
- 2) delete, if existing, any other set of security associations towards this UE immediately; and
- 3) use the kept newly established set of security associations for further messages sent towards the UE.

NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2-1.

Table 5.2.2-1: Handling of security associations at the P-CSCF

	Temporary set of security associations	Newly established set of security associations	Old set of security associations
SIP message received over newly established set of security associations that have not yet been taken into use	No action	Take into use	Reduce SIP level lifetime to $64 \cdot T1$, if lifetime is larger than $64 \cdot T1$
SIP message received over old set of security associations	No action	No action	No action
Old set of security associations currently in use will expire in $64 \cdot T1$	No action	Take into use	No action
Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request	Create Remove any previously existing temporary set of security associations	No action	No action
Sending 200 (OK) response for REGISTER request that concludes re-authentication	Change to a newly established set of security associations	Convert to and treat as old set of security associations (see next column)	Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received. Delete all other old sets of security associations immediately
Sending 200 (OK) response for REGISTER request that concludes initial authentication	Change to a newly established set of security associations and take into use immediately	Convert to old set of security associations, i.e. delete	Delete

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.228 CR 138** ⌘ rev **1** ⌘ Current version: **5.12.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ SDP representation of AMR		
Source:	⌘ Lucent Technologies		
Work item code:	⌘ IMS-CCR	Date:	⌘ 07/04/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<i>Use one of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use one of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ The representation for AMR in SDP in 3GPP TS 24.228 contains a number of inaccuracies, not least the usage of a non-existent attribute "a=maxframes". This is corrected in a manner consistent with the SA4 release 5 specifications for the usage of AMR. Note that the release 6 version of the SA4 specifications have been enhanced with later capabilities, and therefore release 6 examples, if needed, would be different.
Summary of change:	⌘ SDP of the form: a=rtpmap:97 AMR a=fmtp:97 mode-set=0,2,5,7; maxframes=2 a=rtpmap:96 telephone-event is replaced by a=rtpmap:97 AMR a=fmtp:97 mode-set=0,2,5,7;mode-change-period=2 a=rtpmap:96 telephone-event a=maxptime:20 throughout the document
Consequences if not approved:	⌘ The examples represent undefined protocol. Implementations following the examples will not interoperate with conformant implementations.

Clauses affected: ⌘ 7.2.2.1, 7.2.3.1, 7.2.4.1, 7.3.2.1, 7.3.5.1, 7.3.6.1, 7.3.7.1, 7.4.2.1, 7.4.3.1, 7.4.4.1, ⌘

7.4.5.1, 7.4.7.1, 7.4.9.2, 7.4.9.3, 7.5.3, 10.1.2, 10.1.3, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.4.2, 10.4.3, 10.4.4, 10.4.7, 10.5.2, 17.2.2.1, 17.3.2.1, 17.3.3.1, 17.3.4.1, 17.4.2.1, 17.4.5.1, 17.5.2

Other specs affected:		<table border="1"><tr><td>Y</td><td>N</td></tr><tr><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr></table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘	
	Y	N											
	<input type="checkbox"/>	<input checked="" type="checkbox"/>											
<input type="checkbox"/>	<input checked="" type="checkbox"/>												
<input type="checkbox"/>	<input checked="" type="checkbox"/>												
		Test specifications											
		O&M Specifications											
Other comments:	⌘												

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

PROPOSED CHANGE

7.2.2.1 (MO#1a) Mobile origination, roaming (S-S#1a, MT#1a assumed)

Figure 7.2.2.1-1 shows an origination procedure which applies to roaming subscribers when the home network operator does not desire to keep its internal configuration hidden from the visited network. The UE is located in a visited network, and determines the P-CSCF via the CSCF discovery procedure. During registration, the home network allocates a S-CSCF. The home network provides the S-CSCF name/address as the entry point from the visited network.

When registration is complete, P-CSCF knows the name/address of the S-CSCF.

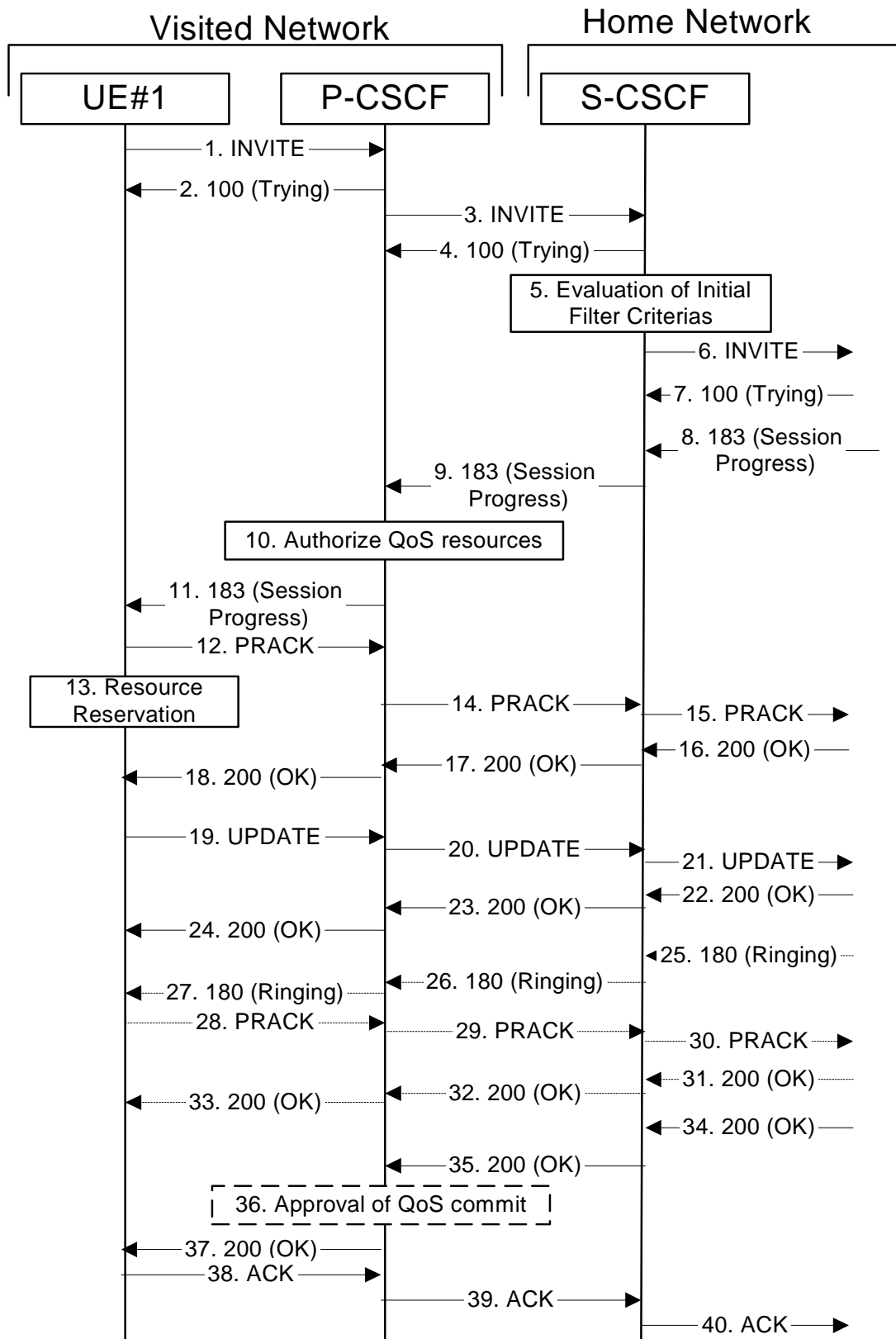


Figure 7.2.2.1-1: MO#1a

Procedure MO#1a is as follows:

- 1. INVITE (UE to P-CSCF) - see example in table 7.2.2.1-1

UE#1 determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for each possible media flow. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.

For this example, it is assumed that UE#1 is willing to establish a multimedia session comprising a video stream and an audio stream. The video stream supports two codecs, either H.263 or MPEG-4 Visual. The audio stream supports the AMR codec.

UE sends the INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism. The initial SDP may represent one or more media for a multimedia session.

Table 7.2.2.1-1: INVITE (UE to P-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
    port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

Request-URI: contains the international E.164 number from the user.

Via: contains the IP address or FQDN of the originating UE.

Route: contains the P-CSCF address learnt during P-CSCF discovery, plus the elements from the Service-Route header from registration. The P-CSCF URI contains the port number learnt during the security agreement negotiation

Privacy: the user does not require privacy, therefore the Privacy header is set to the value “none” as specified in RFC 3325 [17] and RFC 3323 [13].

- P-Preferred-Identity:** the user provides a hint about the identity to be used for this session.
- P-Access-Network-Info:** the UE provides the access-type and access-info, related to the serving access network.
- From:** the user does not require privacy, the From header contains the value requested by the user.
- Cseq:** is a random starting number.
- Security-Verify:** Contains the security agreement as represented by the received Security-Server header.
- Contact:** is a SIP URI that contains the IP address or FQDN of the originating UE.
- SDP** The SDP contains a set of codecs supported by UE#1 and desired by the user at UE#1 for this session.

Upon receiving the INVITE, the P-CSCF stores the following information about this session, for use in possible error recovery actions - see example in table 7.2.2.1-1b.

Table 7.2.2.1-1b: Storage of information at P-CSCF

```
Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq(2dest): 127 INVITE
Cseq(2orig): none
Route(2dest): <sip:scscf1.home1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

2. 100 Trying (P-CSCF to UE) - see example in table 7.2.2.1-2

P-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.2.2.1-2: 100 Trying (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. INVITE (P-CSCF to S-CSCF) - see example in table 7.2.2.1-3

The P-CSCF adds itself to the Record-Route header and Via header. As the request is forwarded to an interface that is not compressed, the own P-CSCF SIP URI does not contain the "comp=sigcomp" parameter.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

The INVITE request is forwarded to the S-CSCF.

Table 7.2.2.1-3: INVITE (P-CSCF to S-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Require: precondition
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Asserted-Identity: P-CSCF inserts the SIP URI in the P-Asserted-Identity header field and it also removes P-Preferred-Identity header field.

P-Access-Network-Info: this header contains information from the UE

P-Charging-Vector: The P-CSCF inserts this header and populates the icid parameters with a globally unique value.

Upon receiving the INVITE, the S-CSCF stores the following information about this session, for use in charging or possible error recovery actions - see example in table 7.2.2.1-3b.

Table 7.2.2.1-3b: Storage of information at S-CSCF

```

Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq(2dest): 127 INVITE
Cseq(2orig): none
Route(2orig): <sip:pcscf1.visited1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

4. 100 Trying (S-CSCF to P-CSCF) - see example in table 7.2.2.1-4

S-CSCF responds to the INVITE request (3) with a 100 Trying provisional response.

Table 7.2.2.1-4: 100 Trying (S-CSCF to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

5. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber and evaluates the initial filter criterias.

6. INVITE (MO#1 to S-S) - see example in table 7.2.2.1-6

S-CSCF forwards the INVITE request, as specified by the S-CSCF to S-CSCF procedures. As the S-CSCF does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

Table 7.2.2.1-6: INVITE request (MO#1a to S-S)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Asserted-Identity: The S-CSCF inserts the corresponding TEL URL to the P-Asserted-Identity header in order that the TEL URL is known to the destination network in case the INVITE is forwarded to a MGCF.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the originating Inter Operator Identifier (IOI) parameter of this header.

Request-URI: In the case where the Request-URI of the incoming INVITE request to S-CSCF contains a TEL-URL [5], it has to be translated to a globally routable SIP-URL before applying it as Request-URI of the outgoing INVITE request. For this address translation the S-CSCF uses the services of an ENUM-DNS protocol according to RFC 2916 [6], or any other suitable translation database. Database aspects of ENUM are outside the scope of this specification.

7. 100 Trying (S-S to MO#1a) - see example in table 7.2.2.1-7 (related to table 7.2.2.1-6)

S-CSCF receives a 100 Trying provisional response, as specified by the S-CSCF to S-CSCF procedures.

Table 7.2.2.1-7: 100 Trying (S-S to MO#1a)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

8. 183 Session Progress (S-S to MO#1a) - see example in table 7.2.2.1-8 (related to table 7.2.2.1-6)

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response (to 6), per the S-CSCF to S-CSCF procedures.

Table 7.2.2.1-8: 183 Session Progress (S-S to MO#1a)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>, <tel:+1-212-555-2222>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net;
    term-ioi=home2.net
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

Upon receiving the 183 Session Progress, the S-CSCF stores the following information about this session, for use in providing enhanced services, charging or in possible error recovery actions – see example in table 7.2.2.1-8b.

Table 7.2.2.1-8b: Storage of information at S-CSCF

```

Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): <sip:scscf2.home2.net;lr>,<sip:pcscf2.visited2.net;lr>
Route(2orig): <sip:pcscf1.visited1.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

9. 183 Session Progress (S-CSCF to P-CSCF) - see example in table 7.2.2.1-9

S-CSCF forwards the 183 Session Progress response to P-CSCF.

Table 7.2.2.1-9: 183 Session Progress (S-CSCF to P-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcsf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Upon receiving the 183 Session Progress, the P-CSCF saves the information as shown in table 7.2.2.1-9b.

Table 7.2.2.1-9b: Storage of information at P-CSCF

```

Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): <sip:scsf1.home1.net;lr>, <sip:scsf2.home2.net;lr>,
  <sip:pcsf2.visited2.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

10. Authorize QoS Resources

P-CSCF authorizes the resources necessary for this session. The approval of QoS commitment either happens at this stage or after 200 OK of INVITE (35) based on operator local policy.

11. 183 Session Progress (P-CSCF to UE) – see example in table 7.2.2.1-11

P-CSCF forwards the 183 Session Progress response to the originating endpoint.

Table 7.2.2.1-11: 183 Session Progress (P-CSCF to UE)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>
P-Asserted-Identity:
Privacy:
P-Media-Authorization:
  0020000100100101706466322e76697369746564322e6e6574000c020139425633303732
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Media-Authorization: a P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf2.visited2.net" with credentials "9BV3072". "00" at the end of the authorization token is required to pad to a multiple of 4 bytes.

Record-Route: The P-CSCF rewrites the Record-Route header to add the port number negotiated during the security agreement and the comp=sigcomp parameter to its own SIP URI.

12. PRACK (UE to P-CSCF) - see example in table 7.2.2.1-12

UE#1 determines which media flows should be used for this session, and which codecs should be used for each of those media flows. If there was any change in media flows, or if there was more than one choice of codec for a media flow, then UE#1 includes a new SDP offer in the PRACK message sent to UE#2.

For this example, assume UE#1 chooses H.263 as the codec to use for the single video stream. Therefore, UE#1 sends a new SDP offer in the PRACK request.

Table 7.2.2.1-12: PRACK (UE to P-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
<sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 128 PRACK
Require: precondition, sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642; port-s=7531
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

Request-URI: takes the value of the Contact header of the received 183 Session Progress response.

Via: takes the value of either the IP address or FQDN of the originating UE.

From:/To:/Call-ID: copied from the 183 Session Progress response so that they include any tag parameter.

Cseq: takes a higher value than that in the previous request.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

13. Resource Reservation

After determining the final media streams in step #11, UE initiates the reservation procedures for the resources needed for this session.

14. PRACK (P-CSCF to S-CSCF) – see example in table 7.2.2.1-14

The P-CSCF forwards the PRACK request to S-CSCF.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

Table 7.2.2.1-14: PRACK (P-CSCF to S-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require: precondition
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

15. PRACK (MO#1a to S-S) – see example in table 7.2.2.1-15

S-CSCF forwards the PRACK request to the terminating endpoint, as per the S-CSCF to S-CSCF procedure.

Table 7.2.2.1-15: PRACK (MO#1a to S-S)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

16. 200 OK (S-S to MO#1a) – see example in table 7.2.2.1-16 (related to table 7.2.2.1-15)

The destination endpoint responds to the PRACK request (14) with a 200 OK response, per the S-CSCF to S-CSCF procedures.

Table 7.2.2.1-16: 200 OK (S-S to MO#1a)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

17. 200 OK (S-CSCF to P-CSCF) - see example in table 7.2.2.1-17

S-CSCF forwards the 200 OK response to P-CSCF.

Table 7.2.2.1-17: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

18. 200 OK (P-CSCF to UE) - see example in table 7.2.2.1-18

P-CSCF forwards the 200 OK response to UE.

Table 7.2.2.1-18: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

19. UPDATE (UE to P-CSCF) – see example in table 7.2.2.1-19

When the resource reservation is completed, UE sends the UPDATE request to the terminating endpoint, via the signalling path established by the INVITE request.

Table 7.2.2.1-19: UPDATE (UE to P-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
<sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 129 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

Request-URI: takes the value of the Contact header of the received 183 Session Progress response.

Via: takes the value of either the IP address or FQDN of the originating UE.

From:/To:/Call-ID: copied from the 183 Session Progress response so that they include any tag parameters.

Cseq: takes a higher value than that in the previous request.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

The SDP indicates that the resource reservation was successful in the local segment.

20. UPDATE (P-CSCF to S-CSCF) – see example in table 7.2.2.1-20

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

P-CSCF forwards the UPDATE request to S-CSCF.

Table 7.2.2.1-20: UPDATE (P-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024";
    ggsn=[5555::4b4:3c3:2d2:1e1]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-
    sig=no; gcid= A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no;
    gcid=F312D5E3BC; flow-id=({2,1},{2,2})"
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Charging-Vector: The P-CSCF added the GPRS access network information to this header, which is removed and stored by the S-CSCF.

Upon receiving the UPDATE, the S-CSCF stores the following information about this session, for use in charging - see example in table 7.2.2.1-20b.

Table 7.2.2.1-20b: Storage of information at S-CSCF

```

Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq(2dest): 127 INVITE
Cseq(2orig): none
Route(2orig): <sip:pcscf1.visited1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>

```

21. UPDATE (MO#1a to S-S) - see example in table 7.2.2.1-21

S-CSCF forwards the UPDATE request to the terminating endpoint, as per the S-CSCF to S-CSCF procedure.

Table 7.2.2.1-21: UPDATE (MO#1a to S-S)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

22. 200 OK (S-S to MO#1a) – see example in table 7.2.2.1-22 (related to table 7.2.2.1-21)

The destination endpoint responds to the UPDATE request (21) with a 200 OK, per the S-CSCF to S-CSCF procedures.

Table 7.2.2.1-22: 200 OK (S-S to MO#1a)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

The SDP indicates that the resource reservation was successful both in the local and the remote segment.

23. 200 OK (S-CSCF to P-CSCF) - see example in table 7.2.2.1-23

S-CSCF forwards the 200 OK response to P-CSCF.

Table 7.2.2.1-23: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

24. 200 OK (P-CSCF to UE) – see example in table 7.2.2.1-24

The P-CSCF forwards the 200 (OK) response to UE.

Table 7.2.2.1-24: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Remainder of subclause not shown

PROPOSED CHANGE

7.2.3.1 (MO#2) Mobile origination, located in home network (S-S#2, MT#2 assumed)

Figure 7.2.3.1-1 shows an origination procedure which applies to subscribers located in their home service area.

The UE is located in the home network, and determines the P-CSCF via the CSCF discovery procedure. During registration, the home network allocates an S-CSCF in the home network.

When registration is complete, the P-CSCF knows the name/address of S-CSCF.

NOTE: Although S-S#2 flow is assumed, home2.net is used in the Record-Route and Route headers in order to be more generic and clearly identify the originating and terminating nodes. In the S-S#2 scenario home2.net = home1.net.

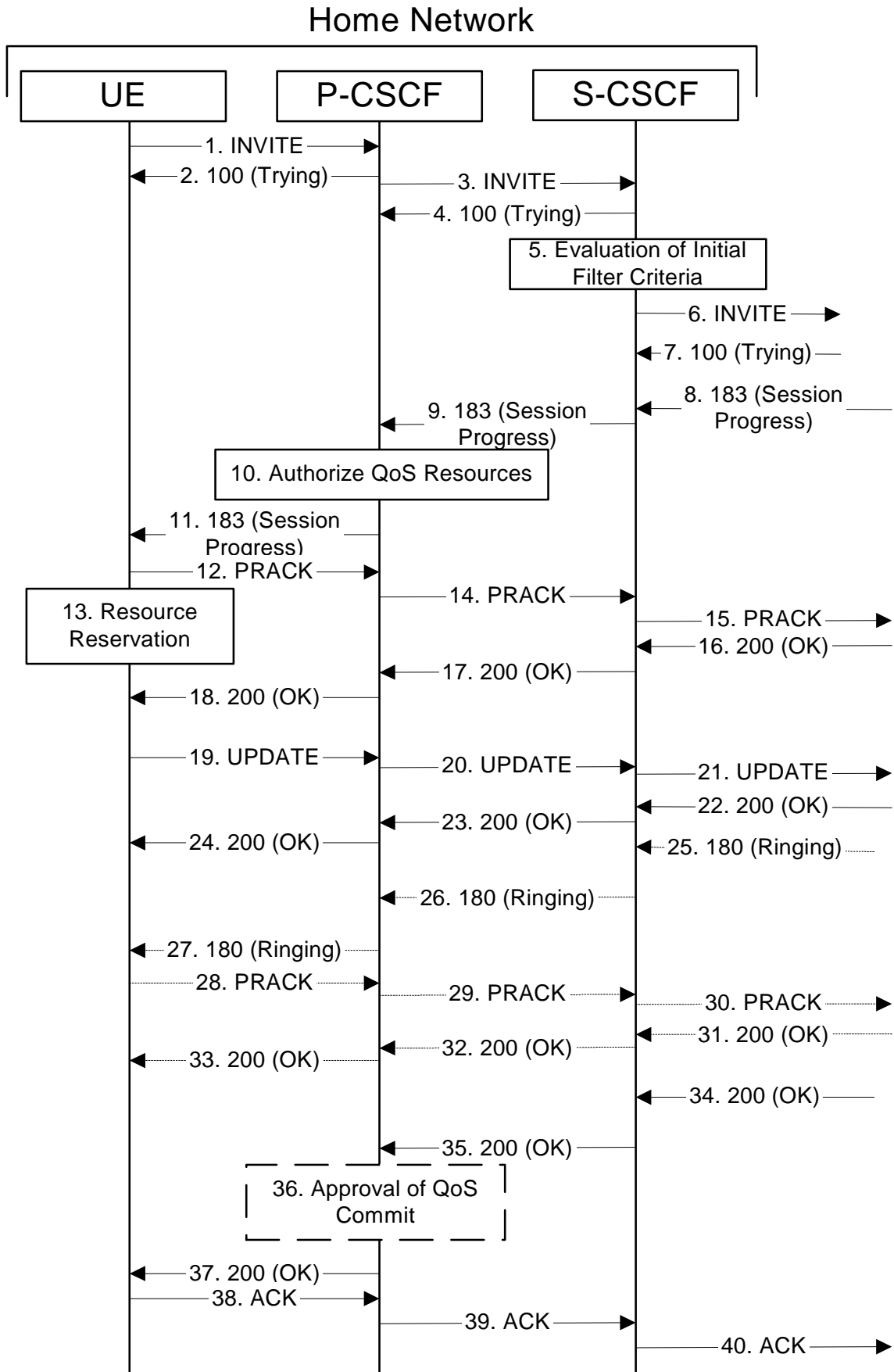


Figure 7.2.3.1-1: MO#2

Procedure MO#2 is as follows:

1. INVITE (UE to P-CSCF) - see example in table 7.2.3.1-1

UE#1 determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for each possible media flow. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.

For this example, it is assumed that UE#1 is willing to establish a multimedia session comprising a video stream and an audio stream. The video stream supports two codecs, either H.263 or MPEG-4 Visual. The audio stream supports the AMR codec.

UE sends the INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism.

Table 7.2.3.1-1: INVITE (UE to P-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
    port-c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

Request-URI: Contains the international E.164 number from the user. This is specified by the UE as <tel:E.164_number>. This is in accordance to standard IETF procedures for specifying dialled digits.

Via: contains the IP address or FQDN of the originating UE.

Route: contains the P-CSCF address learnt during P-CSCF discovery, including the port number negotiated during the security agreement, plus the elements from the Service-Route header from registration.

P-Preferred-Identity: The user provides a hint about the identity to be used for this session.

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

Cseq: A random starting number.

Contact: is a SIP URI that contains the IP address or FQDN of the originating UE. It also contains the port number where the UE wants to receive protected messages.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

SDP The SDP contains a set of codecs supported by UE#1 and desired by the user at UE#1 for this session.

Upon receiving the INVITE, the P-CSCF stores the following information about this session, for use in possible error recovery actions – see example in table 7.2.3.1-1b:

Table 7.2.3.1-1b: Storage of information at P-CSCF

```
Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq(2dest): 127 INVITE
Cseq(2orig): none
Route(2dest): <sip:scscf1.home1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

2. 100 Trying (P-CSCF to UE) – see example in table 7.2.3.1-2

P-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.2.3.1-2: 100 Trying (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. INVITE (P-CSCF to S-CSCF) – see example in table 7.2.3.1-3

The P-CSCF adds itself to the Record-Route header and Via header.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

The INVITE request is forwarded to the S-CSCF.

Table 7.2.3.1-3: INVITE (P-CSCF to S-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Record-Route: <sip:pcscf1.home1.net;lr>
Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Require: precondition
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Asserted-Identity: P-CSCF inserts the TEL URI in the P-Asserted-Identity header field and it also removes P-Preferred-Identity header field.

P-Access-Network-Info: This header contains information from the UE.

P-Charging-Vector: The P-CSCF inserts this header and populates the icid parameters with a unique globally value.

Upon receiving the INVITE, the S-CSCF stores the following information about this session, for use in charging or possible error recovery actions – see example in table 7.2.3.1-3b:

Table 7.2.3.1-3b: Storage of information at S-CSCF

```

Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
Cseq(2orig): none
Route(2orig): <sip:pcscf1.home1.net;lr>
Contact (orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

4. 100 Trying (S-CSCF to P-CSCF) - see example in table 7.2.3.1-4

S-CSCF responds to the INVITE request (3) with a 100 Trying provisional response.

Table 7.2.3.1-4: 100 Trying (S-CSCF to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

5. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias.

6. INVITE (MO#2 to S-S) – see example in table 7.2.3.1-6

S-CSCF forwards the INVITE request, as specified by the S-CSCF to S-CSCF procedures. As the S-CSCF does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

Table 7.2.3.1-6: INVITE (MO#2 to S-S)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-
    ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```


Request-URI: In the case where the Request-URI of the incoming INVITE request to S-CSCF contains a TEL-URL [5], it has to be translated to a globally routable SIP-URL before applying it as Request-URI of the outgoing INVITE request. For this address translation the S-CSCF uses the services of an ENUM-DNS protocol according to RFC 2916 [6], or any other suitable translation database. Database aspects of ENUM are outside the scope of this specification.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the originating Inter Operator Identifier (IOI) parameter of this header.

7. 100 Trying (S-S to MO#2) – see example in table 7.2.3.1-7

S-CSCF receives a 100 Trying provisional response, as specified by the S-CSCF to S-CSCF procedures.

Table 7.2.3.1-7: 100 Trying (S-S to MO#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

8. 183 Session Progress (S-S to MO#2) – see example in table 7.2.3.1-8

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response (to (6)), per the S-CSCF to S-CSCF procedures.

Table 7.2.3.1-8: 183 Session Progress (S-S to MO#2)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.home2.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Smith" <tel:+1-212-555-2222>
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"; orig-ioi=home1.net;
    term-ioi=home2.net
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

Upon receiving the 183 Session Progress, the S-CSCF stores the following information about this session, for use in providing enhanced services, charging or in possible error recovery actions – see example in table 7.2.3.1-8b.

Table 7.2.3.1-8b: Storage of information at S-CSCF

```
Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
Route(2orig): <sip:pcscf1.home1.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

9. 183 Session Progress (S-CSCF to P-CSCF) – see example in table 7.2.3.1-9

S-CSCF forwards the 183 Session Progress response to P-CSCF.

Table 7.2.3.1-9: 183 Session Progress (S-CSCF to P-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Upon receiving the 183 Session Progress, the P-CSCF saves the information as shown in table 7.2.3.1-9b:

Table 7.2.3.1-9b: Storage of information at P-CSCF

```

Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:pcscf2.home2.net;lr>
Contact (dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact (orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

10. Authorize QoS Resources

P-CSCF authorizes the resources necessary for this session. The approval of QoS commitment either happens at this stage or after 200 OK of INVITE (35) based on operator local policy.

11. 183 Session Progress (P-CSCF to UE) – see example in table 7.2.3.1-11

P-CSCF forwards the 183 Session Progress response to the originating endpoint.

Table 7.2.3.1-11: 183 Session Progress (P-CSCF to UE)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>
P-Media-Authorization:
    0020000100100101706466312e686f6d65312e6e6574000c02013942563330373200
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Media-Authorization: a P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf1.home1.net" with credentials "9BV3072". "00" at the end of the authorization token is required to pad to a multiple of 4 bytes.

Record-Route: The P-CSCF rewrites the Record-Route header to add the port number negotiated during the security agreement and the comp=sigcomp parameter to its own SIP URI.

12. PRACK (UE to P-CSCF) – see example in table 7.2.3.1-12

UE#1 determines which media flows should be used for this session, and which codecs should be used for each of those media flows. If there was any change in media flows, or if there was more than one choice of codec for a media flow, then UE#1 include a new SDP offer in the PRACK request sent to UE#2).

For this example, assume UE#1 chooses H.263 as the codec to use for the single video stream. Therefore, UE#1 sends a new SDP offer in the PRACK request.

Table 7.2.3.1-12: PRACK (UE to P-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
      <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 128 PRACK
Require: precondition, sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
      port-c=8642; port-s=7531
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

- Request-URI:** Takes the value of the Contact header of the received 183 Session Progress response.
- Via:** Takes the value of either the IP address or FQDN of the originating UE.
- From:/To:/Call-ID:** Copied from the 183 Session Progress response so that they include any tag parameter.
- Cseq:** Takes a higher value than that in the previous request.
- Security-Verify:** Contains the security agreement as represented by the received Security-Server header.

13. Resource Reservation

After determining the final media streams in step #11, UE initiates the reservation procedures for the resources needed for this session.

14. PRACK (P-CSCF to S-CSCF) – see example in table 7.2.3.1-14

The P-CSCF forwards the PRACK request to S-CSCF.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

Table 7.2.3.1-14: PRACK (P-CSCF to S-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Require: precondition
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

15. PRACK (MO#2 to S-S) – see example in table 7.2.3.1-15

S-CSCF forwards the PRACK request to the terminating endpoint, as per the S-CSCF to S-CSCF procedure.

Table 7.2.3.1-15: PRACK (MO#2 to S-S)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

16. 200 OK (S-S to MO#2) – see example in table 7.2.3.1-16

The destination endpoint responds to the PRACK request (14) with a 200 OK response, per the S-CSCF to S-CSCF procedures.

Table 7.2.3.1-16: 200 OK (S-S to MO#2)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

17. 200 OK (S-CSCF to P-CSCF) – see example in table 7.2.3.1-17

S-CSCF forwards the 200 OK response to P-CSCF.

Table 7.2.3.1-17: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

18. 200 OK (P-CSCF to UE) – see example in table 7.2.3.1-18

P-CSCF forwards the 200 OK response to UE.

Table 7.2.3.1-18: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

19. UPDATE (UE to P-CSCF) – see example in table 7.2.3.1-19

When the resource reservation is completed, UE sends the UPDATE request to the terminating endpoint, via the signalling path established by the INVITE request. The request is sent first to P-CSCF.

Table 7.2.3.1-19: UPDATE (UE to P-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
      <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq: 129 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
      port-c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

Request-URI: Takes the value of the Contact header of the received 183 Session Progress response.

Via: Takes the value of either the IP address or FQDN of the originating UE.

From:/To:/Call-ID: Copied from the 183 Session Progress response so that they include any tag parameters.

CSeq: Takes a higher value than that in the previous request.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

The SDP indicates that the resource reservation was successful in the local segment.

20. UPDATE (P-CSCF to S-CSCF) – see example in table 7.2.3.1-20

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

The P-CSCF forwards the UPDATE request to S-CSCF.

Table 7.2.3.1-20: UPDATE (P-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024";
    ggsn=[5555::4b4:3c3:2d2:1e1]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-
    sig=no; gcid=A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no;
    gcid=F312D5E3BC; flow-id=({2,1},{2,2})"
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Upon receiving the UPDATE, the S-CSCF stores the following information about this session, for use in charging - see example in table 7.2.3.1-20b.

Table 7.2.3.1-20b: Storage of information at S-CSCF

```

Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq(2dest): 127 INVITE
Cseq(2orig): none
Route(2orig): <sip:pcscf1.visited1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>

```

21. UPDATE (MO#2 to S-S) – see example in table 7.2.3.1-21

S-CSCF forwards the UPDATE request to the terminating endpoint, as per the S-CSCF to S-CSCF procedure.

Table 7.2.3.1-21: UPDATE (MO#2 to S-S)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

22. 200 OK (S-S to MO#2) – see example in table 7.2.3.1-22

The destination endpoint responds to the UPDATE request (21) with a 200 OK, per the S-CSCF to S-CSCF procedures.

Table 7.2.3.1-22: 200 OK (S-S to MO#2)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

The SDP indicates that the resource reservation was successful both in the local and the remote segment.

23. 200 OK (S-CSCF to P-CSCF) – see example in table 7.2.3.1-23

S-CSCF forwards the 200 OK response to P-CSCF.

Table 7.2.3.1-23: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

24. 200 OK (P-CSCF to UE) – see example in table 7.2.3.1-24

P-CSCF forwards the 200 OK response to UE.

Table 7.2.3.1-24: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Remainder of subclause not shown

PROPOSED CHANGE

7.2.4.1 CS Networks originated sessions routed towards IM CN subsystem (through MGCF) (S-S#2, MT#2 assumed)

This clause and figure 7.2.4.1-1 presents only the case of CS Networks originated sessions routed towards the IM CN subsystem reaching first a MGCF.

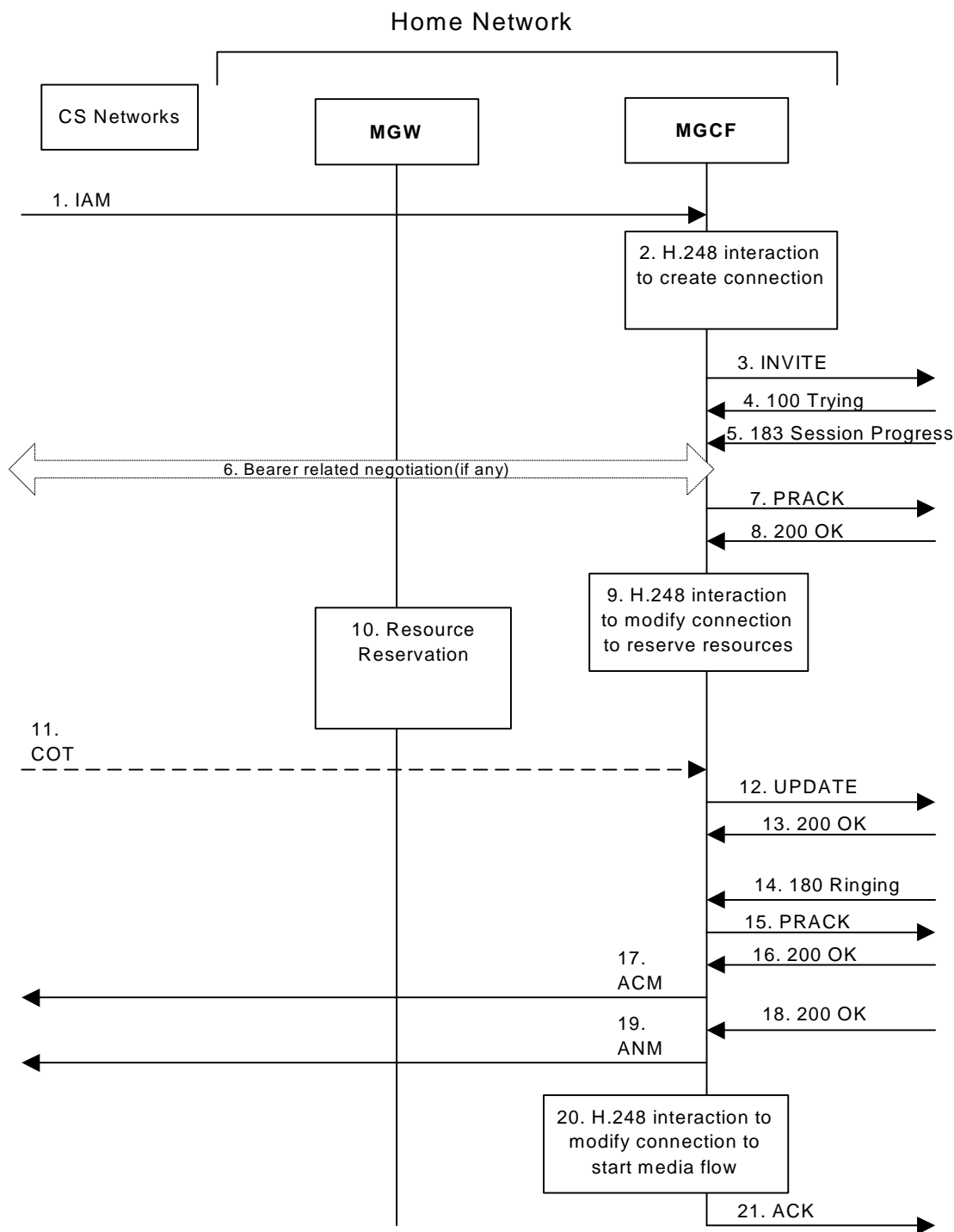


Figure 7.2.4.1-1: CS Networks origination

The CS Networks Origination procedure is as follows:

1. SS7: IAM

The CS Network establishes a bearer path to the MGW, and signals to the MGCF with a IAM message, giving the trunk identity, destination information and optionally the continuity indication.

2. H.248 Interaction

The MGCF initiates a H.248 command, to seize the trunk and an IP port.

3. INVITE (CS-O to S-S) – see example in table 7.2.4.1-3

The MGCF initiates an INVITE request, containing an initial SDP, as per the proper S-CSCF to S-CSCF procedure.

Table 7.2.4.1-3: INVITE (CS-O to S-S)

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP mgcf1.home1.net;branch=z9hG4bK779s24.0
Max-Forwards: 70
Route: <sip:icscf1_s.home1.net;lr>
P-Asserted-Identity: <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <tel:+1-212-555-1111>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:mgcf1.home1.net>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

Request-URI:	Contains the international E.164 number from the user, as obtained from CS Networks signalling.
Via:	Contains the IP address or FQDN of the originating MGCF.
P-Asserted-Identity:	The MGCF inserts the TEL URL containing the subscriber number, as received from the CS network.
P-Charging-Vector:	The MGCF inserts this header and populates the icid parameters with a globally unique value.
Cseq:	A random starting number.
Contact:	Is the SIP URI that contains the IP address or FQDN of the MGCF.
SDP	The SDP contains a preconfigured set of codecs supported by the MGW.

4. 100 Trying (S-S to CS-O) – see example in table 7.2.4.1-4

MGCF receives a 100 Trying provisional response, as specified by the S-CSCF to S-CSCF procedures.

Table 7.2.4.1-4: 100 Trying (S-S to CS-O)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP mgcf1.homel.net;branch=z9hG4bK779s24.0
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

5. 183 Session Progress (S-S to CS-O) – see example in table 7.2.4.1-5

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response, per the S-CSCF to S-CSCF procedures.

Table 7.2.4.1-5: 183 Session Progress (S-S to CS-O)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP mgcf1.homel.net;branch=z9hG4bK779s24.0
Record-Route: <sip:pcscf2.homel.net;lr>, <sip:scscf2.homel.net;lr>
P-Asserted-Identity: "John Smith" <tel:+1-212-555-2222>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=homel.net;
    term-ioi=visitl.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
    ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2;maxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
```

P-Charging-Function-Addresses: The S-CSCF passes this header to the MGCF for charging.

Upon receiving the 183 Session Progress, the MGCF stores the following information about this session – see example in table 7.2.4.1-6b.

Table 7.2.4.1-6b: Storage of information at MGCF

```
Request-URI: tel:+1-212-555-2222
From: <tel:+1-212-555-1111>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 127 INVITE
Route: <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
```

6. Possible bearer related negotiation takes place

Steps 6 and 7 can be done in an arbitrary order.

7. PRACK (CS-O to S-S) – see example in table 7.2.4.1-7

MGCF sends a PRACK request without SDP, because there is not another set of codecs to the original SDP offer.

Table 7.2.4.1-7: PRACK (CS-O to S-S)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP mgcf1.home1.net;branch=z9hG4bK779s24.0
Max-Forwards: 70
Route: <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
From: <tel:+1-212-555-1111>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 128 PRACK
Require: preconditions
RAck: 9021 127 INVITE
Content-Length: 0
```

Via: Takes the value of either the IP address or FQDN of the originating MGCF.

From:/To:/Call-ID: Copied from the 183 Session Progress response so that they include any tag parameter.

Cseq: Takes a higher value than that in the previous request.

8. 200 OK (S-S to CS-O) – see example in table 7.2.4.1-8

The destination responds to the PRACK request (7) with a 200 OK response.

Table 7.2.4.1-8: 200 OK (S-S to CS-O)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP mgcf1.home1.net;branch=z9hG4bK779s24.0
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

9. H.248 Interaction

MGCF initiates a H.248 command to modify the connection parameters and instruct the MGW to reserve the resources needed for the session.

10. Reserve Resources

MGW reserves the resources needed for the session.

11. COT

In case the IAM had contained a continuity indication, the COT message arrives to the MGCF.

12. UPDATE (CS-O to S-S) – see example in table 7.2.4.1-12

When the resource reservation is completed and the possible COT message is received, MGCF sends the UPDATE request to the terminating endpoint, per the S-S procedures.

Table 7.2.4.1-12: UPDATE (CS-O to S-S)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP mgcf1.home1.net;branch=z9hG4bK779s24.0
Max-Forwards: 70
Route: <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
From: <tel:+1-212-555-1111>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
```

Via: Contains the IP address or FQDN of the originating MGCF.

Route: Takes the saved Route header without the first component.

From:/To:/Call-ID: Copied from the 183 Session Progress response so that they include any tag parameters.

Cseq: Takes a higher value than that in the previous request.

The SDP indicates that the resource reservation was successful in the local segment.

13. 200 OK (S-S to CS-O) – see example in table 7.2.4.1-13

The destination endpoint responds to the UPDATE request (12) with a 200 OK response.

Table 7.2.4.1-13: 200 OK (S-S to CS-O)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP mgcf1.home1.net;branch=z9hG4bK779s24.0
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

The SDP indicates that the resource reservation was successful both in the local and the remote segment.

Remainder of subclause not shown

PROPOSED CHANGE

7.3.2.1 (S-S#1a) Different network operators performing origination and termination (MO#1a, MT#1a assumed)

Figure 7.3.2.1-1 shows a S-CSCF handling session origination (S-CSCF#1), which performs an analysis of the destination address, and determines that it belongs to a subscriber of a different operator. The originating network operator does not desire to keep their configuration hidden, so it forwards the request to a well-known entry point in the destination operator's network, I-CSCF. I-CSCF queries the HSS for current location information, and finds the S-CSCF assigned to the subscriber (S-CSCF#2), and forwards the request to S-CSCF#2. The terminating network operator does not desire to keep their configuration hidden, so the I-CSCF does not insert itself into the signalling path for future exchanges. This example flow does not show Application Server involvement.

Origination sequences that share this common S-CSCF to S-CSCF procedure are:

- MO#1a** Mobile origination, roaming, without a THIG. The "Originating Network" of S-S#1a is therefore a visited network.
- MO#1b** Mobile origination, roaming, with a THIG in home network. The "Originating Network" of S-S#1a is therefore a visited network.
- MO#2** Mobile origination, located in home service area. The "Originating Network" of S-S#1a is therefore the home network.

Termination sequences that share this common S-CSCF to S-CSCF procedure are:

- MT#1a** Mobile termination, roaming, without a THIG. The "Terminating Network" of S-S#1a is a visited network.
- MT#1b** Mobile termination, roaming, with a THIG in home network. The "Terminating Network" of S-S#1a is a visited network.
- MT#2** Mobile termination, located in home service area. The "Terminating Network" of S-S#1a is the home network.

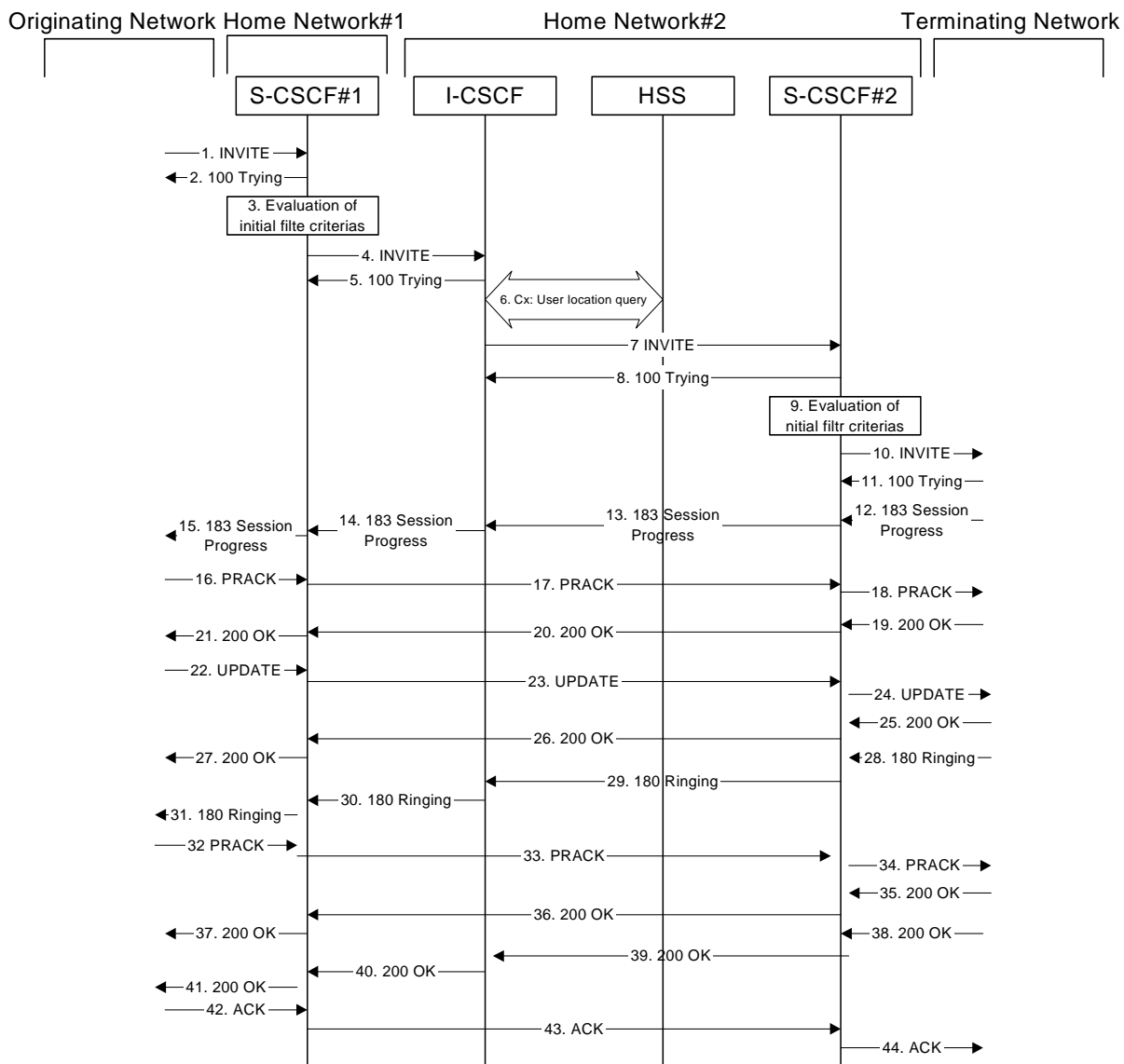


Figure 7.3.2.1-1: S-S#1a

Procedure S-S#1a is as follows:

1. INVITE (MO to S-S#1a) – see example in table 7.3.2.1-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 7.3.2.1-1: INVITE (MO to S-S#1a)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcsf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scsf1.home1.net;lr>
Record-Route: <sip:pcsf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (S-S#1a to MO) – see example in table 7.3.2.1-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.3.2.1-2: 100 Trying (S-S#1a to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcsf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias. For this example, assume no Application Server involvement.

4. INVITE (S-CSCF to I-CSCF) – see example in table 7.3.2.1-4

S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since the originating operator does not desire to keep their internal configuration hidden, S-CSCF#1 forwards the INVITE request directly to to I-CSCF in the destination network.

As the S-CSCF does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

Table 7.3.2.1-4: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Request-URI: In the case where the Request-URI of the incoming INVITE request to S-CSCF contains a TEL-URL [5], it has to be translated to a globally routable SIP-URL before applying it as Request-URI of the outgoing INVITE request. For this address translation the S-CSCF uses the services of an ENUM-DNS protocol according to RFC 2916 [6], or any other suitable translation database. Database aspects of ENUM are outside the scope of this specification.

P-Asserted-Identity: The S-CSCF adds the corresponding TEL URL to the P-Asserted-Identity header in order that the TEL URL is known to the destination network in case the INVITE is forwarded to a MGCF.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the originating Inter Operator Identifier (IOI) parameter of this header.

5. 100 Trying (I-CSCF to S-CSCF) – see example in table 7.3.2.1-5

I-CSCF responds to the INVITE request (4) by sending a 100 Trying provisional response to S-CSCF#1.

Table 7.3.2.1-5: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228 [11].

Table 6.3.2-6a provides the parameters in the SIP INVITE request (flow 4), which are sent to the HSS.

Table 7.3.2.1-6a Cx: User registration status query procedure (I-CSCF to HSS)

Message source & destination	Cx: Information element name	Information source in SIP INVITE	Description
I-CSCF to HSS	User Public Identity	Request-URI:	This information element indicates the public user identity

Table 7.3.2.1-6b provides the parameters sent from the HSS that need to be mapped to SIP INVITE (flow 7) and sent to S-CSCF.

Table 7.3.2.1-6b Cx: User registration status query procedure (HSS to I-CSCF)

Message source & destination	Cx: Information element name	Mapping to SIP header in SIP INVITE	Description
HSS to I-CSCF	S-CSCF name	Route header field	This information indicates the serving CSCF's name of that user

7. INVITE (I-CSCF to S-CSCF) – see example in table 7.3.2.1-7

I-CSCF forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

Table 7.3.2.1-7: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

NOTE: The I-CSCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

8. 100 Trying (S-CSCF to I-CSCF) – see example in table 7.3.2.1-8

S-CSCF#2 responds to the INVITE request (7) with a 100 Trying provisional response.

Table 7.3.2.1-8: 100 Trying (S-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

9. Evaluation of initial filter criterias

S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criterias.

10. INVITE (S-S#1a to MT) – see example in table 7.3.2.1-10

S-CSCF#2 forwards the INVITE request, as determined by the termination procedure. S-CSCF#2 remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE.

Table 7.3.2.1-10: INVITE (S-S#1a to MT)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (...)

```

```

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

11. 100 Trying (MT to S-S#1a) – see example in table 7.3.2.1-11 (related to table 7.3.2.1-10)

S-CSCF#2 receives a 100 Trying provisional response to the INVITE request (10), as specified by the termination procedures.

Table 7.3.2.1-11: 100 Trying (MT to S-S#1a)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

12. 183 Session Progress (MT to S-S#1a) – see example in table 7.3.2.1-12 (related to table 7.3.2.1-10)

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response to the INVITE request (10), as per the termination procedure.

Table 7.3.2.1-12: 183 Session Progress (MT to S-S#1a)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

13. 183 Session Progress (S-CSCF to I-CSCF) – see example in table 7.3.2.1-13

S-CSCF#2 forwards the 183 Session Progress provisional response to I-CSCF.

Table 7.3.2.1-13: 183 Session Progress (S-CSCF to I-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>, <tel:+1-212-555-2222>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Asserted-Identity: The S-CSCF adds the corresponding TEL URL to the P-Asserted-Identity header in order that the TEL URL is known to the destination network in case the INVITE is forwarded to a MGCF.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the terminating Inter Operator Identifier (IOI) parameter of this header.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

14. 183 Session Progress (I-CSCF to S-CSCF) – see example in table 7.3.2.1-14

I-CSCF forwards the 183 Session Progress provisional response to S-CSCF#1.

Table 7.3.2.1-14: 183 Session Progress (I-CSCF to S-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

15. 183 Session Progress (S-S#1a to MO) – see example in table 7.3.2.1-15

S-CSCF#1 forwards the 183 Session Progress to the originator, as per the originating procedure.

Table 7.3.2.1-15: 183 Session Progress (S-S#1a to MO)

SIP/2.0 183 Session Progress Via: SIP/2.0/UDP pscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7 Record-Route: P-Asserted-Identity: P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024" Privacy: From: To: Call-ID: CSeq: Require: Contact: Allow: RSeq: Content-Type: Content-Length: v= o= s= c= t= m= b= a= a= a= a= a= a= a= a= a= a= m= b= a= a= a= a= a= a= a= a= a= a= a=
--

16. PRACK (MO to S-S#1a) – see example in table 7.3.2.1-16

The originator decides the final set of media streams, and includes this information in the PRACK request sent to S-CSCF#1 by the origination procedures.

Table 7.3.2.1-16: PRACK (MO to S-S#1a)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:cscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 128 PRACK
Require: precondition
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

17. PRACK (S-CSCF to S-CSCF) – see example in table 7.3.2.1-17

S-CSCF#1 forwards the PRACK request to S-CSCF#2.

Table 7.3.2.1-17: PRACK (S-CSCF to S-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

18. PRACK (S-S#1a to MT) – see example in table 7.3.2.1-18

S-CSCF#2 forwards the PRACK request to the terminating endpoint, as per the termination procedure.

Table 7.3.2.1-18: PRACK (S-S#1a to MT)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

19. 200 OK (MT to S-S#1a) – see example in table 7.3.2.1-19 (related to table 7.3.2.1-18)

The terminating endpoint responds to the PRACK request (18) with a 200 OK response.

Table 7.3.2.1-19: 200 OK (MT to S-S#1a)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

20. 200 OK (S-CSCF to S-CSCF) – see example in table 7.3.2.1-20

S-CSCF#2 forwards the 200 OK response to S-CSCF#1.

Table 7.3.2.1-20: 200 OK (S-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

21. 200 OK (S-S#1a to MO) – see example in table 7.3.2.1-21

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 7.3.2.1-21: 200 OK (S-S#1a to MO)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscfl.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

22. UPDATE (MO to S-S#1a) – see example in table 7.3.2.1-22

When the originating endpoint has completed the resource reservation procedures, it sends the UPDATE request to S-CSCF#1 by the origination procedures.

Table 7.3.2.1-22: UPDATE (MO to S-S#1a)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024";
  ggsn=[5555::4b4:3c3:2d2:1e1]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-
  sig=no; gcid=A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no;
  gcid=F312D5E3BC; flow-id=({2,1},{2,2})"
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdEgIkJ490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

23. UPDATE (S-CSCF to S-CSCF) – see example in table 7.3.2.1-23

S-CSCF#1 forwards the UPDATE request to S-CSCF#2.

Table 7.3.2.1-23: UPDATE (S-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
term-ioi=home2.net
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

24. UPDATE (S-S#1a to MT) – see example in table 7.3.2.1-24

S-CSCF#2 forwards the UPDATE request to the terminating endpoint, as per the termination procedure.

Table 7.3.2.1-24: UPDATE (S-S#1a to MT)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.visited2.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

25. 200 OK (MT to S-S#1a) – see example in table 7.3.2.1-25 (related to table 7.3.2.1-24)

The terminating endpoint responds to the UPDATE request (24) with a 200 OK response.

Table 7.3.2.1-25: 200 OK (MT to S-S#1a)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
      scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
      pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

26. 200 OK (S-CSCF to S-CSCF) – see example in table 7.3.2.1-26

S-CSCF#2 forwards the 200 OK response to S-CSCF#1.

Table 7.3.2.1-26: 200 OK (S-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

27. 200 OK (S-S#1a to MO) – see example in table 7.3.2.1-27

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 7.3.2.1-27: 200 OK (S-S#1a to MO)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Remainder of subclause not shown

PROPOSED CHANGE

7.3.5.1 (S-S#2) Single network operator performing origination and termination (MO#2, MT#2 assumed)

Figure 7.3.5.1-1 shows a S-CSCF handling session origination, which performs an analysis of the destination address, and determines that it belongs to a subscriber of the same operator. The request is therefore forwarded to a local I-CSCF. The I-CSCF queries the HSS for current location information, and finds the S-CSCF assigned to the subscriber (S-CSCF#2), and forwards the request to S-CSCF#2.

Origination sequences that share this common S-CSCF to S-CSCF procedure are:

- MO#1a** Mobile origination, roaming, without a THIG. The "Originating Network" of S-S#2 is therefore a visited network.
- MO#1b** Mobile origination, roaming, with a THIG in home network. The "Originating Network" of S-S#2 is therefore a visited network.
- MO#2** Mobile origination, located in home service area. The "Originating Network" of S-S#2 is therefore the home network.
- CS-O** CS Networks origination. The "Originating Network" of S-S#2 is the home network. The element labeled S-CSCF#1 is the MGCF of the CS-O procedure with the exception that all actions performed by the labelled S-CSCF#1 handling the session origination will not be performed by the MGCF: It does not perform the evaluation of initial filter criteria and the destination address translation. The details of the flow do not show the CS-O case..

Termination sequences that share this common S-CSCF to S-CSCF procedure are:

- MT#1a** Mobile termination, roaming, without a THIG. The "Terminating Network" of S-S#2 is a visited network.
- MT#1b** Mobile termination, roaming, with a THIG in home network. The "Terminating Network" of S-S#2 is a visited network.
- MT#2** Mobile termination, located in home service area. The "Terminating Network" of S-S#2 is the home network.

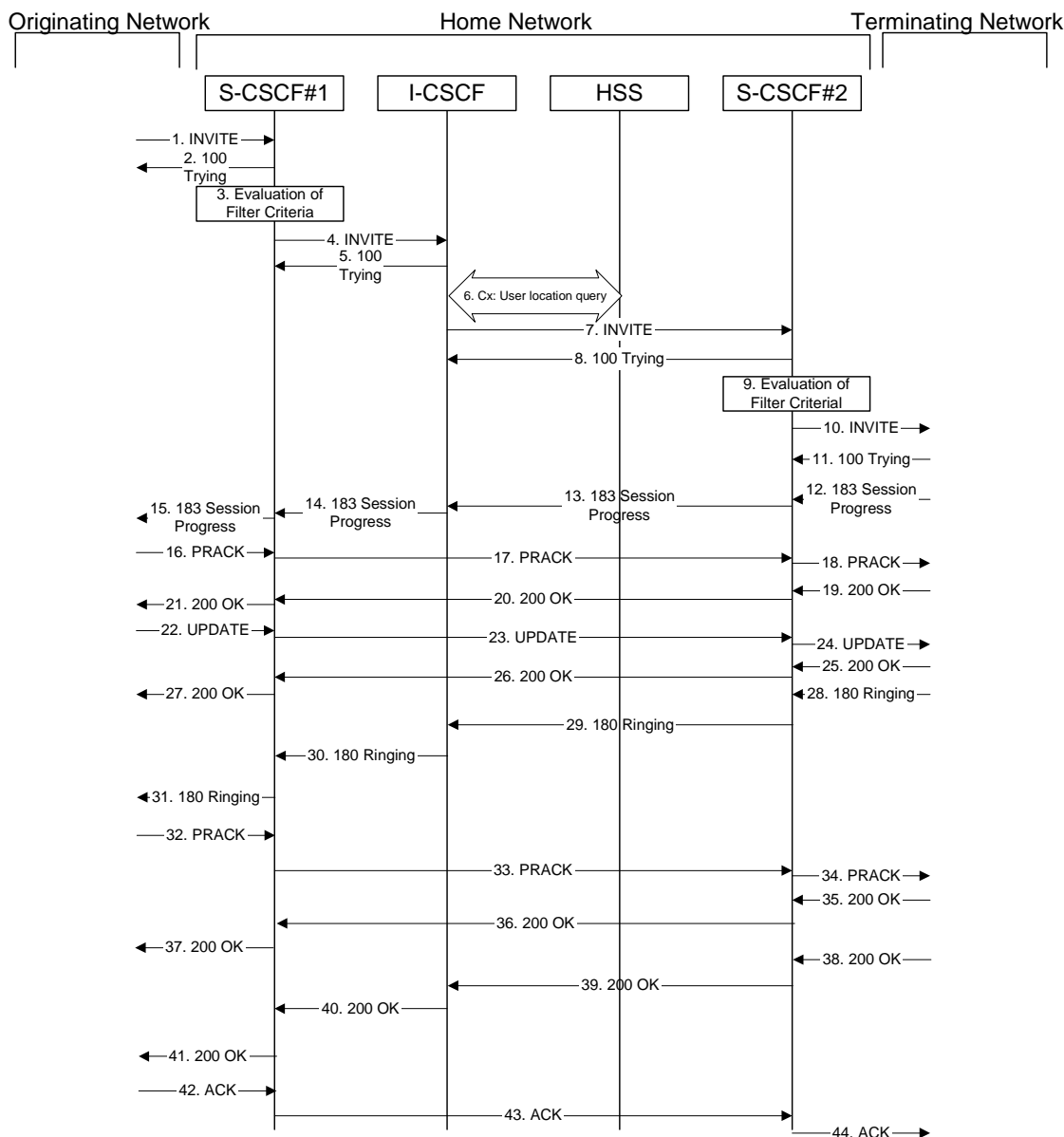


Figure 7.3.5.1-1: S-S#2

Procedure S-S#2 is as follows:

1. INVITE (MO to S-S#2) – see example in table 7.3.5.1-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 7.3.5.1-1: INVITE (MO to S-S#2)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (S-S#2 to MO) – see example in table 7.3.5.1-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.3.5.1-2: 100 Trying (S-S#2 to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias. For this example, assume no Application Server involvement.

4. INVITE (S-CSCF to I-CSCF) – see example in table 7.3.5.1-4

S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since the originating operator does not desire to keep their internal configuration hidden, S-CSCF#1 forwards the INVITE request directly to I-CSCF in the destination network.

As the S-CSCF knows that the next hop I-CSCF is in the same home network (and therefore, a loose router), it includes a Route header.

Table 7.3.5.1-4: INVITE (S-CSCF to I-CSCF)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
      pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:icscf2_s.home1.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Request-URI: In the case where the Request-URI of the incoming INVITE request to S-CSCF contains a TEL-URL [5], it has to be translated to a globally routable SIP-URL before applying it as Request-URI of the outgoing INVITE request. For this address translation the S-CSCF uses the services of an ENUM-DNS protocol according to RFC 2916 [6], or any other suitable translation database. Database aspects of ENUM are outside the scope of this specification.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the originating Inter Operator Identifier (IOI) parameter of this header.

5. 100 Trying (I-CSCF to S-CSCF) – see example in table 7.3.5.1-5

I-CSCF responds to the INVITE request (4) by sending a 100 Trying provisional response to S-CSCF#1.

Table 7.3.5.1-5: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228[11].

Table 7.3.2.1-6a provides the parameters in the SIP INVITE request (flow 4), which are sent to the HSS.

Table 7.3.2.1-6b provides the parameters sent from the HSS that need to be mapped to SIP INVITE request (flow 7) and sent to S-CSCF.

7. INVITE (I-CSCF to S-CSCF) – see example in table 7.3.5.1-7

I-CSCF forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

Table 7.3.5.1-7: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home1.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Supported:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

NOTE: The I-CSCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

8. 100 Trying (S-CSCF to I-CSCF) – see example in table 7.3.5.1-8

S-CSCF#2 responds to the INVITE request (8) with a 100 Trying provisional response.

Table 7.3.5.1-8: 100 Trying (S-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

9. Evaluation of initial filter criterias

S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criterias.

10. INVITE (S-S#2 to MT) – see example in table 7.3.5.1-10

S-CSCF#2 forwards the INVITE request, as determined by the termination procedure. S-CSCF#2 remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE.

Table 7.3.5.1-10: INVITE (S-S#2 to MT)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
     icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.home1.net;lr>
Record-Route: <sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>,
              <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
P-Called-Party-ID: <sip:user2_public1@home1.net>
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

11. 100 Trying (MT to S-S#2) – see example in table 7.3.5.1-11 (related to table 7.3.5.1-10)

S-CSCF#2 receives a 100 Trying provisional response to the INVITE request (11), as specified by the termination procedures.

Table 7.3.5.1-11: 100 Trying (MT to S-S#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

12. 183 Session Progress (MT to S-S#2) – see example in table 7.3.5.1-12 (related to table 7.3.5.1-10)

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response, as per the termination procedure.

Table 7.3.5.1-12: 183 Session Progress (MT to S-S#2)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP icscf2_s.home1.net,
    SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.home1.net;lr>, <sip:scscf2.home1.net;lr>,
    <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Smith" <tel:+1-212-555-2222>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

13. 183 Session Progress (S-CSCF to I-CSCF) – see example in table 7.3.5.1-13

S-CSCF#2 forwards the 183 Session Progress provisional response to I-CSCF.

Table 7.3.5.1-13: 183 Session Progress (S-CSCF to I-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
    term-ioi=home1.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
    ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the terminating Inter Operator Identifier (IOI) parameter of this header.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

14. 183 Session Progress (I-CSCF to S-CSCF) – see example in table 7.3.5.1-14

I-CSCF forwards the 183 Session Progress provisional response to S-CSCF#1.

Table 7.3.5.1-14: 183 Session Progress (I-CSCF to S-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:
```

```
v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

15. 183 Session Progress (S-S#2 to MO) – see example in table 7.3.5.1-15

S-CSCF#1 forwards the 183 Session Progress to the originator, as per the originating procedure.

Table 7.3.5.1-15: 183 Session Progress (S-S#2 to MO)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

16. PRACK (MO to S-S#2) – see example in table 7.3.5.1-16

The originator decides the final set of media streams, and includes this information in the PRACK request sent to S-CSCF#1 by the origination procedures.

Table 7.3.5.1-16: PRACK (MO to S-S#2)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 128 PRACK
Require: precondition
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

17. PRACK (S-CSCF to S-CSCF) – see example in table 7.3.5.1-17

S-CSCF#1 forwards the PRACK request to S-CSCF#2.

Table 7.3.5.1-17: PRACK (S-CSCF to S-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

18. PRACK (S-S#2 to MT) – see example in table 7.3.5.1-18

S-CSCF#2 forwards the PRACK request to the terminating endpoint, as per the termination procedure.

Table 7.3.5.1-18: PRACK (S-S#2 to MT)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

19. 200 OK (MT to S-S#2) – see example in table 7.3.5.1-19 (related to table 7.3.5.1-18)

The terminating endpoint responds to the PRACK request (19) with a 200 OK response.

Table 7.3.5.1-19: 200 OK (MT to S-S#2)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
      scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
      pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

20. 200 OK (S-CSCF to S-CSCF) – see example in table 7.3.5.1-20

S-CSCF#2 forwards the 200 OK response to S-CSCF#1.

Table 7.3.5.1-20: 200 OK (S-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

21. 200 OK (S-S#2 to MO) – see example in table 7.3.5.1-21

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 7.3.5.1-21: 200 OK (S-S#2 to MO)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

22. UPDATE (MO to S-S#2) – see example in table 7.3.5.1-22

When the originating endpoint has completed the resource reservation procedures, it sends the UPDATE request to S-CSCF#1 by the origination procedures.

Table 7.3.5.1-22: UPDATE (MO to S-S#2)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

23. UPDATE (S-CSCF to S-CSCF) – see example in table 7.3.5.1-23

S-CSCF#1 forwards the UPDATE request to S-CSCF#2.

Table 7.3.5.1-23: UPDATE (S-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

24. UPDATE (S-S#2 to MT) – see example in table 7.3.5.1-24

S-CSCF#2 forwards the UPDATE request to the terminating endpoint, as per the termination procedure.

Table 7.3.5.1-24: UPDATE (S-S#2 to MT)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
      scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
      pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

25. **200 OK (MT to S-S#2)** – see example in table 7.3.5.1-25 (related to table 7.3.5.1-24)

The terminating endpoint responds to the UPDATE request (24) with a 200 OK response.

Table 7.3.5.1-25: 200 OK (MT to S-S#2)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
      scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
      pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

26. 200 OK (S-CSCF to S-CSCF) – see example in table 7.3.5.1-26

S-CSCF#2 forwards the 200 OK response to S-CSCF#1.

Table 7.3.5.1-26: 200 OK (S-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

27. 200 OK (S-S#2 to MO) – see example in table 7.3.5.1-27

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 7.3.5.1-27: 200 OK (S-S#2 to MO)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Remainder of subclause not shown

PROPOSED CHANGE

7.3.6.1 (S-S#3) PSTN Termination performed by home network of originator (MO#2 assumed)

Figure 7.3.6.1-1 shows a S-CSCF handling session origination, which performs an analysis of the destination address, and determines that it will result in a PSTN termination. The request is therefore forwarded to a local BGCF. The BGCF performs further analysis of the destination address, combined with information of agreements between operators for optimum Gateway selection, and decides to do the PSTN termination locally. The BGCF therefore allocates a MGCF within the home network, and sends the request to it. This example flow does not show Application Server involvement.

Origination sequences that share this common S-CSCF to S-CSCF procedure are:

- MO#1a** Mobile origination, roaming, without a THIG. The "Originating Network" of S-S#3 is therefore a visited network.
- MO#1b** Mobile origination, roaming, with a THIG in home network. The "Originating Network" of S-S#3 is therefore a visited network.
- MO#2** Mobile origination, located in home service area. The "Originating Network" of S-S#3 is therefore the home network.
- CS-O** CS Networks origination. The "Originating Network" of S-S#3 is the home network. The element labelled S-CSCF#1 is the MGCF of the CS-O procedure.

Termination sequences that share this common S-CSCF to S-CSCF procedure are:

- CS-T** CS Networks termination.

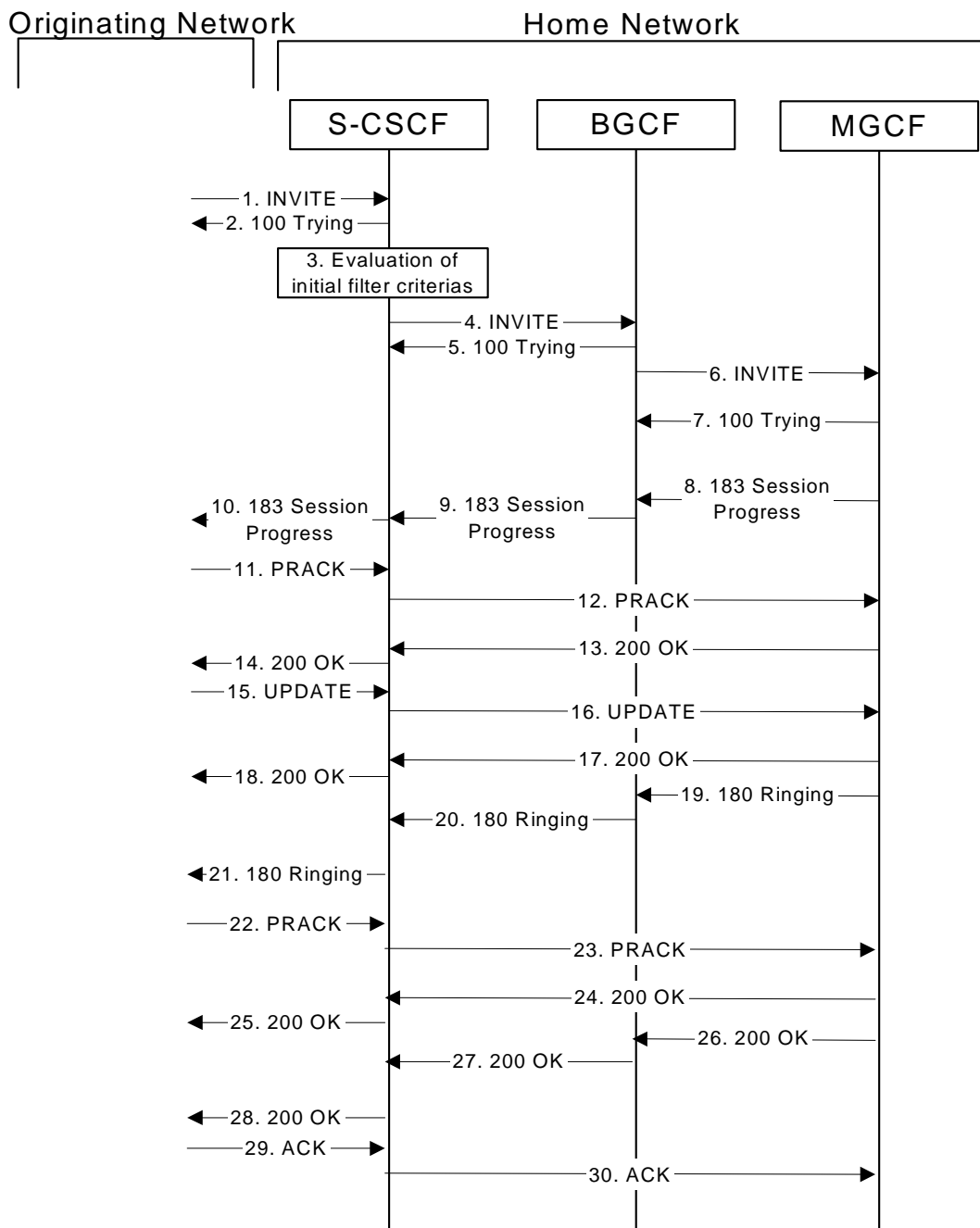


Figure 7.3.6.1-1: S-S#3

Procedure S-S#3 is as follows:

1. INVITE (MO to S-S#3) – see example in table 7.3.6.1-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 7.3.6.1-1: INVITE (MO to S-S#3)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (S-S#3 to MO) – see example in table 7.3.6.1-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.3.6.1-2: 100 Trying (S-S#3 to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias. For this example, assume no Application Server involvement.

4. INVITE (S-CSCF to BGCF) – see example in table 7.3.6.1-4

S-CSCF#1 performs an analysis of the destination address, and determines the destination is on the PSTN. S-CSCF forwards the INVITE request to the BGCF in the local network.

Table 7.3.6.1-4: INVITE (S-CSCF to BGCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:bgcf1.home1.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector:
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
    ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Charging-Vector: The S-CSCF passes this header to the BGCF for charging.

P-Charging-Function-Addresses: The S-CSCF inserts this header to provide the charging function addresses to the BGCF.

5. 100 Trying (BGCF to S-CSCF) – see example in table 7.3.6.1-5

BGCF sends a 100 Trying provisional response to S-CSCF.

Table 7.3.6.1-5: 100 Trying (BGCF to S-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

6. INVITE (BGCF to MGCF) – see example in table 7.3.6.1-6

BGCF analyzes the destination address, and allocates a MGCF to handle the termination. BGCF forwards the INVITE request to the MGCF.

Table 7.3.6.1-6: INVITE (BGCF to MGCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:mgcf1.home1.net;lr>
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
P-Charging-Function-Addresses:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

NOTE: The BGCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

7. 100 Trying (MGCF to BGCF) – see example in table 7.3.6.1-7

MGCF responds to the INVITE request (6) with a 100 Trying provisional response.

Table 7.3.6.1-7: 100 Trying (MGCF to BGCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

8. 183 Session Progress (MGCF to BGCF) – see example in table 7.3.6.1-8

The MGCF returns the media stream capabilities of the destination along the signalling path in a 183 Session Progress provisional response.

Table 7.3.6.1-8: 183 Session Progress (MGCF to BGCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Smith" <tel:+1-212-555-2222>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; term-ioi=home1.net
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:mgcf1.home1.net>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2;maxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
```

9. 183 Session Progress (BGCF to S-CSCF) – see example in table 7.3.6.1-9

BGCF forwards the 183 Session Progress provisional response to S-CSCF.

Table 7.3.6.1-9: 183 Session Progress (BGCF to S-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcopm;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

10. 183 Session Progress (S-S#3 to MO) – see example in table 7.3.6.1-10

S-CSCF#1 forwards the 183 Session Progress to the originator, as per the originating procedure.

Table 7.3.6.1-10: 183 Session Progress (S-S#3 to MO)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

11. PRACK (MO to S-S#3) – see example in table 7.3.6.1-11

The originator confirms with a PRACK request sent to S-CSCF#1 by the origination procedures. The request does not contain SDP because in the initial SDP offer/answer there was a single media stream with a single codec.

Table 7.3.6.1-11: PRACK (MO to S-S#3)

```
PRACK sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 128 PRACK
Require: precondition
RAck: 9021 127 INVITE
Content-Length: 0
```

12. PRACK (S-CSCF to MGCF) – see example in table 7.3.6.1-12

S-CSCF forwards the PRACK request to MGCF.

Table 7.3.6.1-12: PRACK (S-CSCF to MGCF)

```

PRACK sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Length:

```

13. 200 OK (MGCF to S-CSCF) – see example in table 7.3.6.1-13

The MGCF responds to the PRACK request (12) with a 200 OK response.

Table 7.3.6.1-13: 200 OK (MGCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
Content-Length: 0

```

14. 200 OK (S-S#3 to MO) – see example in table 7.3.6.1-14

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 7.3.6.1-14: 200 OK (S-S#3 to MO)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:

```

15. UPDATE (MO to S-S#3) – see example in table 7.3.6.1-15

When the originating endpoint has completed the resource reservation procedures, it sends the UPDATE request to S-CSCF#1 by the origination procedures.

Table 7.3.6.1-15: UPDATE (MO to S-S#3)

```

UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024";
  ggsn=[5555::4b4:3c3:2d2:1e1]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-
  sig=no; gcid=A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no;
  gcid=F312D5E3BC; flow-id=({2,1},{2,2})"
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdFglkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

P-Charging-Vector: The P-CSCF added the GPRS access network information to this header, which is removed and stored by the S-CSCF.

Upon receiving the UPDATE, the S-CSCF stores the P-Charging-Vector information for use in charging.

16. UPDATE (S-CSCF to MGCF) – see example in table 7.3.6.1-16

S-CSCF forwards the UPDATE request to MGCF.

Table 7.3.6.1-16: UPDATE (S-CSCF to MGCF)

```

UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

17. 200 OK (MGCF to S-CSCF) – see example in table 7.3.6.1-17

The MGCF responds to the UPDATE request (16) with a 200 OK response.

Table 7.3.6.1-17: 200 OK (MGCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

18. 200 OK (S-S#3 to MO) – see example in table 7.3.6.1-18

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 7.3.6.1-18: 200 OK (S-S#3 to MO)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

Remainder of subclause not shown

PROPOSED CHANGE

7.3.7.1 (S-S#4) PSTN Termination performed by different operator than origination (MO#2 assumed)

Figure 7.3.7.1-1 shows a S-CSCF handling session origination, which performs an analysis of the destination address, and determines that it will result in a PSTN termination. The request is therefore forwarded to a local BGCF (BGCF#1). BGCF#1 performs further analysis of the destination address, combined with information of agreements between operators for optimum Gateway selection, and decides to do the PSTN termination in a different operator's network. BGCF#1 therefore forwards the request to a BGCF in the terminating operator's network, BGCF#2. BGCF#2 allocates a MGCF within the its network, and sends the request to it. This example flow does not show Application Server involvement.

Origination sequences that share this common S-CSCF to S-CSCF procedure are:

- MO#1a** Mobile origination, roaming, without a THIG. The "Originating Network" of S-S#4 is therefore a visited network.
- MO#1b** Mobile origination, roaming, with a THIG in home network. The "Originating Network" of S-S#4 is therefore a visited network.
- MO#2** Mobile origination, located in home service area. The "Originating Network" of S-S#4 is therefore the home network.
- CS-O** CS Networks origination. The "Originating Network" of S-S#4 is the home network. The element labeled S-CSCF#1 is the MGCF of the CS-O procedure.

Termination sequences that share this common S-CSCF to S-CSCF procedure are:

- CS-T** CS Networks termination.

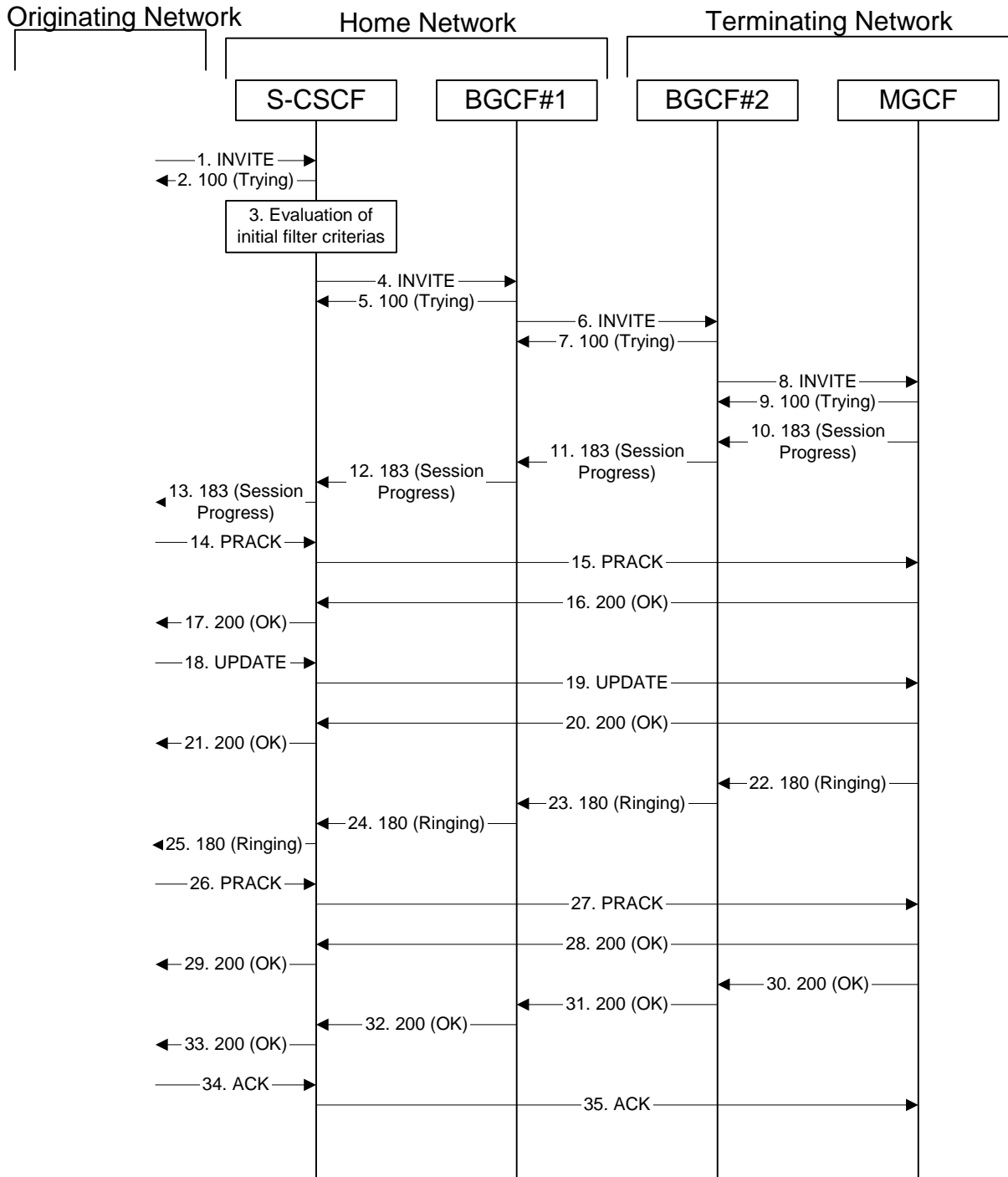


Figure 7.3.7.1-1: S-S#4

Procedure S-S#4 is as follows:

1. INVITE (MO to S-S#4) – see example in table 7.3.7.1-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 7.3.7.1-1: INVITE (MO to S-S#4)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

```

```

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (S-S#4 to MO) – see example in table 7.3.7.1-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.3.7.1-2: 100 Trying (S-S#4 to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias. For this example, assume no Application Server involvement.

4. INVITE (S-CSCF to BGCF) – see example in table 7.3.7.1-4

S-CSCF#1 performs an analysis of the destination address, and determines the destination is on the PSTN. S-CSCF#1 forwards the INVITE request to the BGCF in the local network.

Table 7.3.7.1-4: INVITE (S-CSCF to BGCF)

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:bgcf1.home1.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector:
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
  ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Charging-Vector: The S-CSCF passes this header to the BGCF for charging.

P-Charging-Function-Addresses: The S-CSCF inserts this header to provide the charging function addresses to the BGCF.

5. **100 Trying (BGCF to S-CSCF)** – see example in table 7.3.7.1-5

BGCF#1 sends a 100 Trying provisional response to S-CSCF#1.

Table 7.3.7.1-5: 100 Trying (BGCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. **INVITE (BGCF to BGCF)** – see example in table 7.3.7.1-6

BGCF#1 analyses the destination address, and the inter-operator agreements for optimal PSTN termination, and selects the network operator that can best terminate this session. BGCF#1 forwards the INVITE request to the BGCF (BGCF#2) in the network that will handle the session termination.

Table 7.3.7.1-6: INVITE (BGCF to BGCF)

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:bgcf2.home2.net;lr>
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

7. 100 Trying (BGCF to BGCF) – see example in table 7.3.7.1-7

BGCF#2 responds to the INVITE request (6) with a 100 Trying provisional response.

Table 7.3.7.1-7: 100 Trying (BGCF to BGCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

8. INVITE (BGCF to MGCF) – see example in table 7.3.7.1-8

BGCF#2 allocates a Media Gateway Controller, and forwards the INVITE request to that MGCF.

Table 7.3.7.1-8: INVITE (BGCF to MGCF)

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP bgcf2.home2.net;branch=z9hG4bK456u71.1, SIP/2.0/UDP
  bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
  scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:mgcf2.home2.net;lr>
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

9. 100 Trying (MGCF to BGCF) – see example in table 7.3.7.1-9

MGCF sends a 100 Trying provisional response.

Table 7.3.7.1-9: 100 Trying (MGCF to BGCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP bgcf2.home2.net;branch=z9hG4bK456u71.1, SIP/2.0/UDP
  bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
  scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

10. 183 Session Progress (MGCF to BGCF) – see example in table 7.3.7.1-10

MGCF returns the media stream capabilities of the destination in a 183 Session Progress provisional response.

Table 7.3.7.1-10: 183 Session Progress (MGCF to BGCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP bgcf2.home2.net;branch=z9hG4bK456u71.1, SIP/2.0/UDP
    bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Smith" <tel:+1-212-555-2222>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; term-ioi=home2.net
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:mgcf2.home2.net>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

11. 183 Session Progress (BGCF to BGCF) – see example in table 7.3.7.1-11

BGCF#2 forwards the 183 Session Progress provisional response to BGCF#1.

Table 7.3.7.1-11: 183 Session Progress (BGCF to BGCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

12. 183 Session Progress (BGCF to S-CSCF) – see example in table 7.3.7.1-12

BGCF#1 forwards the 183 Session Progress provisional response to S-CSCF.

Table 7.3.7.1-12: 183 Session Progress (BGCF to S-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

13. 183 Session Progress (S-S#4 to MO) – see example in table 7.3.7.1-13

S-CSCF#1 forwards the 183 Session Progress response to the originator, as per the originating procedure.

Table 7.3.7.1-13: 183 Session Progress (S-S#4 to MO)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

14. PRACK (MO to S-S#4) – see example in table 7.3.7.1-14

The originator sends a PRACK request sent to S-CSCF by the origination procedures. The PRACK request does not contain SDP because in the initial SDP offer/answer the negotiation resulted in a single media stream with a single codec.

Table 7.3.7.1-14: PRACK (MO to S-S#4)

```

PRACK sip:mgcf2.home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 128 PRACK
Require: precondition
RAck: 9021 127 INVITE
Content-Length: 0

```

15. PRACK (S-CSCF to MGCF) – see example in table 7.3.7.1-15

S-CSCF forwards the PRACK request to the MGCF.

Table 7.3.7.1-15: PRACK (S-CSCF to MGCF)

```

PRACK sip:mgcf2.home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Length:

```

16. 200 OK (MGCF to S-CSCF) – see example in table 7.3.7.1-16

The MGCF responds to the PRACK request (15) with a 200 OK response.

Table 7.3.7.1-16: 200 OK (MGCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

17. 200 OK (S-S#4 to MO) – see example in table 7.3.7.1-17

S-CSCF forwards the 200 OK response to the originating endpoint.

Table 7.3.7.1-17: 200 OK (S-S#4 to MO)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:

```

18. UPDATE (MO to S-S#4) – see example in table 7.3.7.1-18

When the originating endpoint has completed the resource reservation procedures, it sends the UPDATE request to S-CSCF#1 by the origination procedures.

Table 7.3.7.1-18: UPDATE (MO to S-S#4)

```

UPDATE sip:mgcf2.home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024";
  ggsn=[5555::4b4:3c3:2d2:1e1]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-
  sig=no; gcid=A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no;
  gcid=F312D5E3BC; flow-id=({2,1},{2,2})"
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdFglkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

P-Charging-Vector: The P-CSCF added the GPRS access network information to this header, which is removed and stored by the S-CSCF.

Upon receiving the UPDATE, the S-CSCF stores the P-Charging-Vector information for use in charging.

19. UPDATE (S-CSCF to MGCF) – see example in table 7.3.7.1-19

S-CSCF forwards the UPDATE request to the MGCF.

Table 7.3.7.1-19: UPDATE (S-CSCF to MGCF)

```

UPDATE sip:mgcf2.home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

20. 200 OK (MGCF to S-CSCF) – see example in table 7.3.7.1-20

The MGCF responds to the UPDATE request (19) with a 200 OK response.

Table 7.3.7.1-20: 200 OK (MGCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmt:97 mode-set=0,2,5,7; mode-change-period;maxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

Remainder of subclause not shown

PROPOSED CHANGE

7.4.2.1 (MT#1a) Mobile termination, roaming (MO#1a, S-S#1a assumed)

Figure 7.4.2.1 shows a termination procedure which applies to roaming subscribers when the home network operator does not desire to keep its internal configuration hidden from the visited network. The UE is located in a visited network, and determines the P-CSCF via the P-CSCF discovery procedure. During registration, the home network allocates the S-CSCF.

When registration is complete, S-CSCF knows the name/address of P-CSCF and the UE Contact address, and P-CSCF obtains the name/address of the UE.

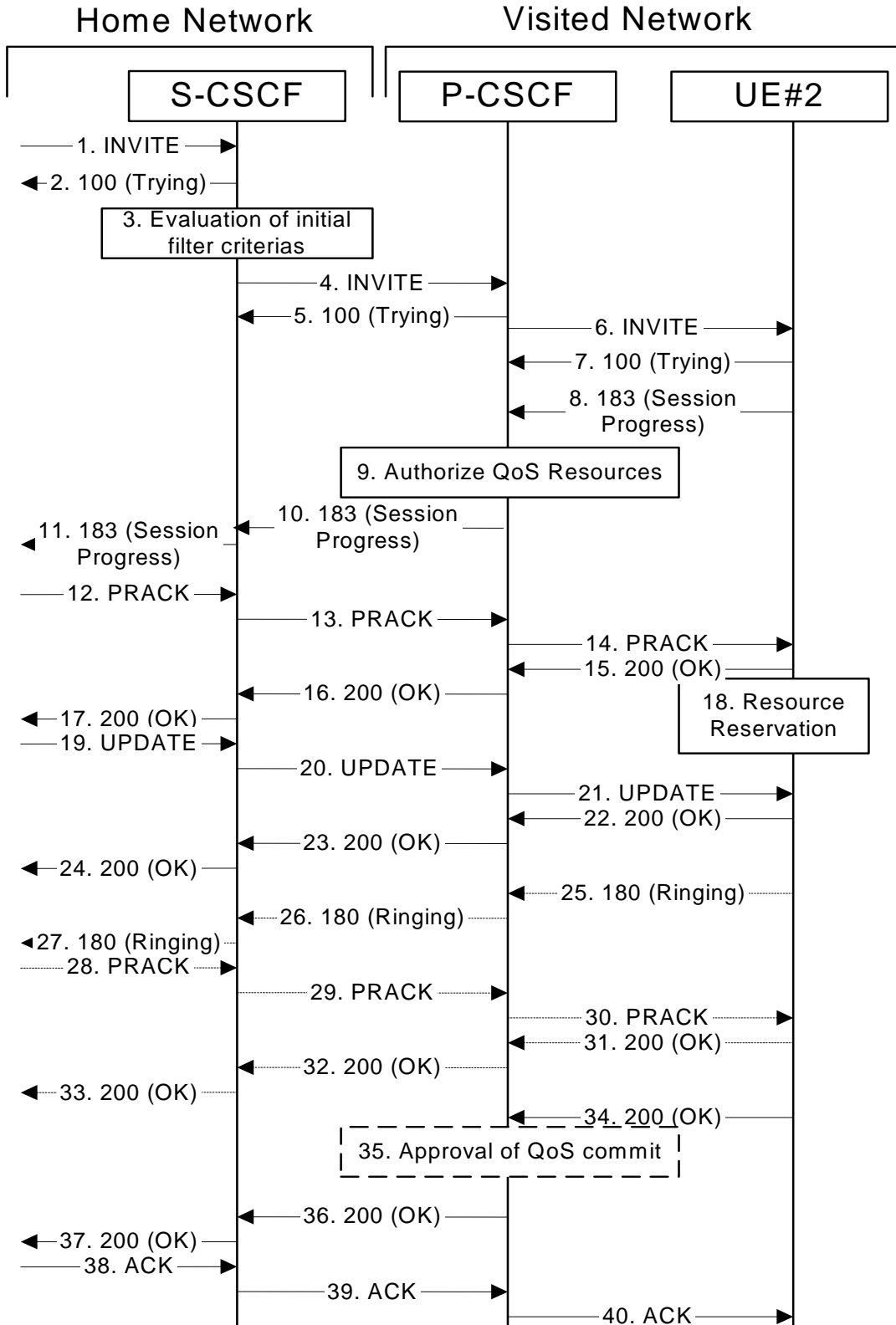


Figure 7.4.2.1-1: MT#1a

Procedure MT#1a is as follows:

1. INVITE (S-S to MT#1a) – see example in table 7.4.2.1-1

The calling party sends the INVITE request, via one of the origination procedures and via one of the S-CSCF to S-CSCF procedures, to the S-CSCF for the terminating subscriber.

Table 7.4.2.1-1: INVITE (S-S to MT#1a)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported:
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
a=rtptime:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

SDP The SDP contains the complete set of supported and desired codecs from the session originator.

Upon receipt of the INVITE, the S-CSCF stores the following information about this session, for use in providing enhanced services, charging or in possible error recovery actions – see example in table 7.4.2.1-1b.

Table 7.4.2.1-1b: Storage of information at S-CSCF

```

Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

2. 100 Trying (MT#1a to S-S) – see example in table 7.4.2.1-2

S-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.4.2.1-2: 100 Trying (MT#1a to S-S)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias.

4. INVITE (S-CSCF to P-CSCF) – see example in table 7.4.2.1-4

S-CSCF remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE. It forwards the INVITE to the P-CSCF.

Table 7.4.2.1-4: INVITE (S-CSCF to P-CSCF)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrblHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (...

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Route: Built from the Path header stored at registration.

P-Called-Party-ID: Includes the dialled URL with its parameters.

Via/Record-Route: S-CSCF adds itself.

P-CSCF saves information from the received INVITE request. The saved value of the information for this session is – see example in table 7.4.2.1-4b.

Table 7.4.2.1-4b: Storage of information at P-CSCF

```
Request-URI: sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfgklkj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.visited1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

5. 100 Trying (P-CSCF to S-CSCF) – see example in table 7.4.2.1-5

P-CSCF responds to the INVITE request (4) with a 100 Trying provisional response.

Table 7.4.2.1-5: 100 Trying (P-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. INVITE (P-CSCF to UE) – see example in table 7.4.2.1-6

Table 7.4.2.1-6: INVITE (P-CSCF to UE)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k2l.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
Privacy:
P-Media-Authorization:
0020000100100101706466312e686f6d65312e6e6574000c02013331533134363231
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
P-Called-Party-ID:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its Via header.

Record-Route: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its own URI.

P-Media-Authorization: A P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf1.home1.net" with credentials "31S14621".

7. 100 Trying (UE to P-CSCF) – see example in table 7.4.2.1-7

UE may optionally send a 100 Trying provisional response to P-CSCF.

Table 7.4.2.1-7: 100 Trying (UE to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcsf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

8. 183 Session Progress (UE to P-CSCF) – see example in table 7.4.2.1-8

UE#2 determines the complete set of codecs that it is capable of supporting for this session. It determines the intersection with those appearing in the SDP in the INVITE request.

UE responds with a 183 Session Progress response containing SDP back to the originator. This response is sent to P-CSCF.

Table 7.4.2.1-8: 183 Session Progress (UE to P-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

To: A tag is added to the To header.

Contact: Contains a SIP URI with the IP address or FQDN of the UE. It includes the comp=sigcomp parameter.

SDP The SDP contains the set of codecs supported by UE. It requests a confirmation of the QoS preconditions for establishing the session

Upon receipt of the 183 Session Progress, the P-CSCF stores the following information about this session, for use in providing enhanced services or in possible error recovery actions – see example in table 7.4.2.1-8b.

Table 7.4.2.1-8b: Storage of information at P-CSCF

```
Request-URI: sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.visited1.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

9. Authorize QoS Resources

P-CSCF authorizes the resources necessary for this session. The approval of QoS commitment either happens at this stage or after 200 OK of INVITE (34) based on operator local policy.

10. 183 Session Progress (P-CSCF to S-CSCF) – see example in table 7.4.2.1-10

P-CSCF forwards the 183 Session Progress response to S-CSCF.

Table 7.4.2.1-10: 183 Session Progress (P-CSCF to S-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7)
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Record-Route: The P-CSCF rewrites the Record-Route header field value to remove the port number used for the security association and the comp=sigcomp parameter from its own URI

P-Asserted-Identity: P-CSCF inserts the default SIP URI of the user in the P-Asserted-Identity header field.

P-Access-Network-Info: this header contains information from the UE.

Upon receipt of the 183 Session Progress, the S-CSCF stores the following information about this session, for use in providing enhanced services or in possible error recovery actions – see example in table 7.4.2.1-10b.

Table 7.4.2.1-10b: Storage of information at S-CSCF

```
Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): <sip:pcscf2.visited2.net;lr>
Route(2orig): <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

11. 183 Session Progress (MT#1a to S-S) – see example in table 7.4.2.1-11

S-CSCF forwards the 183 Session Progress response to the originator, per the S-CSCF to S-CSCF procedure.

Table 7.4.2.1-11: 183 Session Progress (MT#1a to S-S)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>, <tel:+1-212-555-2222>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net;
term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Asserted-Identity: S-CSCF inserts the TEL URI of the user in the P-Asserted-Identity header field.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the terminating Inter Operator Identifier (IOI) parameter of this header and puts back the originating IOI parameter.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

12. PRACK (S-S to MT#1a) – see example in table 7.4.2.1-12

The originating endpoint sends a PRACK request containing the final SDP to be used in this session, via the S-CSCF to S-CSCF procedure, to S-CSCF.

Table 7.4.2.1-12: PRACK (S-S to MT#1a)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 128 PRACK
Require: precondition
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

13. PRACK (S-CSCF to P-CSCF) – see example in table 7.4.2.1-13

S-CSCF forwards the PRACK request to P-CSCF.

Table 7.4.2.1-13: PRACK (S-CSCF to P-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

14. PRACK (P-CSCF to UE) – see example in table 7.4.2.1-14

P-CSCF forwards the PRACK request to UE.

Table 7.4.2.1-14: PRACK (P-CSCF to UE)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsfc2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcsfc1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its own entry in the Via header.

15. 200 OK (UE to P-CSCF) – see example in table 7.4.2.1-15

UE acknowledges the PRACK request (14) with a 200 OK response.

Table 7.4.2.1-15: 200 OK (UE to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

16. 200 OK (P-CSCF to S-CSCF) – see example in table 7.4.2.1-16

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.4.2.1-16: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

17. 200 OK (MT#1a to S-S) – see example in table 7.4.2.1-17

S-CSCF forwards the 200 OK response to the originator, per the S-CSCF to S-CSCF procedure.

Table 7.4.2.1-17: 200 OK (MT#1a to S-S)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

18. Resource Reservation

UE initiates the reservation procedures for the resources needed for this session.

19. UPDATE (S-S to MT#1a) – see example in table 7.4.2.1-19

When the originating endpoint has completed its resource reservation, it sends the UPDATE request to S-CSCF, via the S-CSCF to S-CSCF procedures.

Table 7.4.2.1-19: UPDATE (S-S to MT#1a)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

20. UPDATE (S-CSCF to P-CSCF) – see example in table 7.4.2.1-20

S-CSCF forwards the UPDATE request to P-CSCF.

Table 7.4.2.1-20: UPDATE (S-CSCF to P-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

21. UPDATE (P-CSCF to UE) – see example in table 7.4.2.1-21

P-CSCF forwards the UPDATE request to UE.

Table 7.4.2.1-21: UPDATE (P-CSCF to UE)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: The P-CSCF adds the port number negotiated in the security agreement and the comp=sigcomp parameter to its own entry in the Via header.

22. 200 OK (UE to P-CSCF) – see example in table 7.4.2.1-22

UE acknowledges the UPDATE request (21) with a 200 OK response.

Table 7.4.2.1-22: 200 OK (UE to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscaf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

23. 200 OK (P-CSCF to S-CSCF) – see example in table 7.4.2.1-23

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.4.2.1-23: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

24. 200 OK (MT#1a to S-S) – see example in table 7.4.2.1-24

S-CSCF forwards the 200 OK response to the originator, per the S-CSCF to S-CSCF procedure.

Table 7.4.2.1-24: 200 OK (MT#1a to S-S)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

Remainder of subclause not shown

PROPOSED CHANGE

7.4.3.1 (MT#2) Mobile termination, located in home network (MO#2, S-S#2 assumed)

Figure 7.4.3.1-1 shows a termination procedure which applies to subscribers located in their home service area.

The UE is located in the home network, and determines the P-CSCF via the CSCF discovery procedure. During registration, the home network allocates a S-CSCF in the home network, S-CSCF.

When registration is complete, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE.

NOTE: Although S-S#2 flow is assumed, home2.net is used in the Via, Record-Route and Route headers in order to be more generic and clearly identify the originating and terminating nodes. In the S-S#2 scenario home2.net = home1.net.

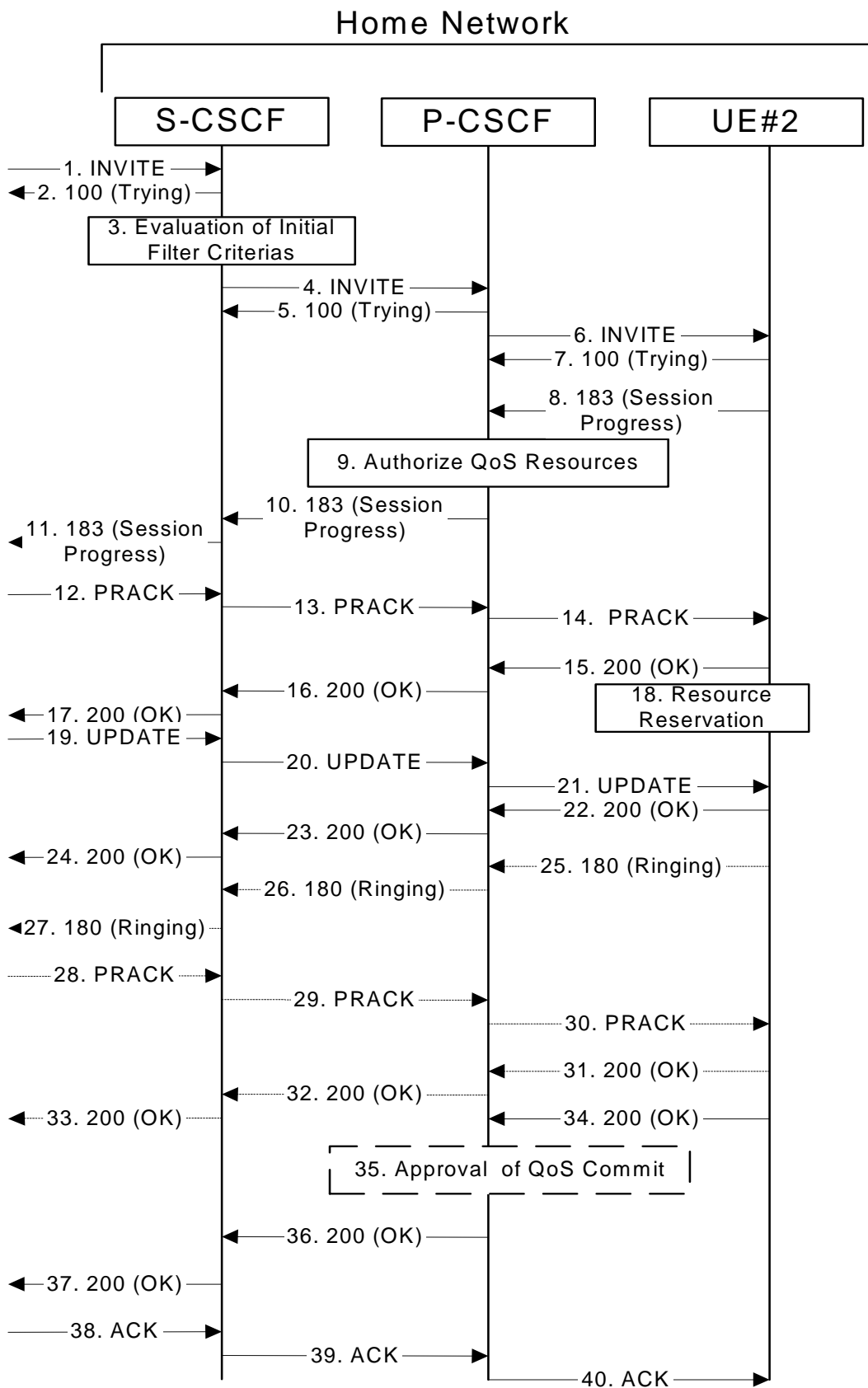


Figure 7.4.3.1-1: MT#2

Procedure MT#2 is as follows:

1. INVITE (S-S to MT#2) – see example in table 7.4.3.1-1

The calling party sends the INVITE request, via one of the origination procedures and via one of the S-CSCF to S-CSCF procedures, to the S-CSCF for the terminating subscriber.

Table 7.4.3.1-1: INVITE (S-S to MT#2)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home1.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 127 INVITE
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:99 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2;maxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

Upon receipt of the INVITE, the S-CSCF stores the following information about this session, for use in providing enhanced services, charging or in possible error recovery actions – see example in table 7.4.3.1-1b.

Table 7.4.3.1-1b: Storage of information at S-CSCF

```
Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

2. 100 Trying (MT#2 to S-S) – see example in table 7.4.3.1-2

S-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.4.3.1-2: 100 Trying (MT#2 to S-S)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias.

4. INVITE (S-CSCF to P-CSCF) – see example in table 7.4.3.1-4

S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE request to the P-CSCF.

Table 7.4.3.1-4: INVITE (S-CSCF to P-CSCF)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.home2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

- Route:** Built from the Path header stored at registration.
- P-Called-Party-ID:** Includes the dialled URL with its parameters.
- Via:, Record-Route:** S-CSCF adds itself in the Record-Route and Via headers.

P-CSCF saves information from the received INVITE request. The saved value of the information for this session is – see example in table 7.4.3.1-4b.

Table 7.4.3.1-4b: Storage of information at P-CSCF

```

Request-URI: sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:pcscf1.home1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

5. 100 Trying (P-CSCF to S-CSCF) – see example in table 7.4.3.1-5

P-CSCF responds to the INVITE request (4) with a 100 Trying provisional response.

Table 7.4.3.1-5: 100 Trying (P-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. INVITE (P-CSCF to UE) – see example in table 7.4.3.1-6

Table 7.4.3.1-6: INVITE (P-CSCF to UE)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Record-Route: <sip:pcscf2.home2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
    <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
P-Called-Party-ID:
P-Media-Authorization:
    0020000100100101706466322e686f6d65312e6e6574000c02013331533134363231
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Media-Authorization: A P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf1.home1.net" with credentials "31S14621".

Record-Route: The P-CSCF adds the port number negotiated in the security agreement and the comp=sigcomp parameter to its own SIP URI.

Via: The P-CSCF adds the port number negotiated in the security agreement and the comp=sigcomp parameter to its own entry.

7. 100 Trying (UE to P-CSCF) – see example in table 7.4.3.1-7

UE may optionally send a 100 Trying provisional response to P-CSCF.

Table 7.4.3.1-7: 100 Trying (UE to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

8. 183 Session Progress (UE to P-CSCF) – see example in table 7.4.3.1-8

UE#2 determines the complete set of codecs that it is capable of supporting for this session. It determines the intersection with those appearing in the SDP in the INVITE request.

UE responds with a 183 Session Progress response containing SDP back to the originator. This response is sent to P-CSCF.

Table 7.4.3.1-8: 183 Session Progress (UE to P-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pscsf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.home2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

To: A tag is added to the To header.

Contact: Contains a SIP URI with the IP address or FQDN of the terminating UE.

SDP The SDP contains the subset of codecs supported by UE. It requests a confirmation of the QoS preconditions for establishing the session.

Upon receipt of the 183 Session Progress, the P-CSCF stores the following information about this session, for use in providing enhanced services or in possible error recovery actions – see example in table 7.4.3.1-8b.

Table 7.4.3.1-8b: Storage of information at P-CSCF

```

Request-URI: sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.home1.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

9. Authorize QoS Resources

P-CSCF authorizes the resources necessary for this session. The approval of QoS commitment either happens at this stage or after 200 OK of INVITE (34) based on operator local policy.

10. 183 Session Progress (P-CSCF to S-CSCF) – see example in table 7.4.3.1-10

P-CSCF forwards the 183 Session Progress response to S-CSCF.

Table 7.4.3.1-10: 183 Session Progress (P-CSCF to S-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7)
Record-Route: <sip:pcscf2.home2.net;lr>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Access-Network-Info:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAfrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Access-Network-Info: This header contains information from the UE.

P-Asserted-Identity: P-CSCF inserts the default SIP URI of the user in the P-Asserted-Identity header field.

Record-Route: The P-CSCF rewrites the Record-Route header to remove the port number and the comp=sigcomp parameter from its own SIP URI

Upon receipt of the 183 Session Progress, the S-CSCF stores the following information about this session, for use in providing enhanced services or in possible error recovery actions – see example in table 7.4.3.1-10b.

Table 7.4.3.1-10b: Storage of information at S-CSCF

```
Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): <sip:pcscf2.home2.net;lr>
Route(2orig): <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

11. 183 Session Progress (MT#2 to S-S) – see example in table 7.4.3.1-11

S-CSCF forwards the 183 Session Progress response to the originator, per the S-CSCF to S-CSCF procedure.

Table 7.4.3.1-11: 183 Session Progress (MT#2 to S-S)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"; orig-ioi=home1.net;
term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the terminating Inter Operator Identifier (IOI) parameter of this header and puts back the originating IOI parameter.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

12. PRACK (S-S to MT#2) – see example in table 7.4.3.1-12

The originating endpoint sends a PRACK request containing the final SDP to be used in this session, via the S-CSCF to S-CSCF procedure, to S-CSCF.

Table 7.4.3.1-12: PRACK (S-S to MT#2)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 128 PRACK
Require: precondition
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

13. PRACK (S-CSCF to P-CSCF) – see example in table 7.4.3.1-13

S-CSCF forwards the PRACK request to P-CSCF.

Table 7.4.3.1-13: PRACK (S-CSCF to P-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

14. PRACK (P-CSCF to UE) – see example in table 7.4.3.1-14

P-CSCF forwards the PRACK request to UE.

Table 7.4.3.1-14: PRACK (P-CSCF to UE)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

15. 200 OK (UE to P-CSCF) – see example in table 7.4.3.1-15

UE acknowledges the PRACK request (14) with a 200 OK response.

Table 7.4.3.1-15: 200 OK (UE to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

16. 200 OK (P-CSCF to S-CSCF) – see example in table 7.4.3.1-16

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.4.3.1-16: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

17. 200 OK (MT#2 to S-S) – see example in table 7.4.3.1-17

S-CSCF forwards the 200 OK response to the originator, per the S-CSCF to S-CSCF procedure.

Table 7.4.3.1-17: 200 OK (MT#2 to S-S)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

18. Resource Reservation

UE initiates the reservation procedures for the resources needed for this session.

19. UPDATE (S-S to MT#2) – see example in table 7.4.3.1-19

When the originating endpoint has completed its resource reservation, it sends the UPDATE request to S-CSCF, via the S-CSCF to S-CSCF procedures.

Table 7.4.3.1-19: UPDATE (S-S to MT#2)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

20. UPDATE (S-CSCF to P-CSCF) – see example in table 7.4.3.1-20

S-CSCF forwards the UPDATE request to P-CSCF.

Table 7.4.3.1-20: UPDATE (S-CSCF to P-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

21. UPDATE (P-CSCF to UE) – see example in table 7.4.3.1-21

P-CSCF forwards the UPDATE request to UE.

Table 7.4.3.1-21: UPDATE (P-CSCF to UE)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

22. 200 OK (UE to P-CSCF) – see example in table 7.4.3.1-22

UE acknowledges the UPDATE request (21) with a 200 OK response.

Table 7.4.3.1-22: 200 OK (UE to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net:5088;branch=z9hG4bK876t12.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

23. 200 OK (P-CSCF to S-CSCF) – see example in table 7.4.3.1-23

P-CSCF forwards the 200 OK response to S-CSCF.

Table 7.4.3.1-23: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

24. 200 OK (MT#2 to S-S) – see example in table 7.4.3.1-24

S-CSCF forwards the 200 OK response to the originator, per the S-CSCF to S-CSCF procedure.

Table 7.4.3.1-24: 200 OK (MT#2 to S-S)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

Remainder of subclause not shown

PROPOSED CHANGE

7.4.4.1 (CS-T) CS Networks termination (MO#2, S-S#3 assumed)

Figure 7.4.4.1-1 shows the MGCF in the IM CN subsystem, which is a SIP endpoint that initiates and receives requests on behalf of the CS Networks and Media Gateway (MGW). Other nodes consider the signalling as if it came from a S-CSCF. The MGCF incorporates the network security functionality of the S-CSCF.

Agreements between network operators may allow CS Networks termination in a network other than the originator's home network. This may be done, for example, to avoid long distance or international tariffs.

This termination procedure can be used in either S-S#3 or S-S#4.

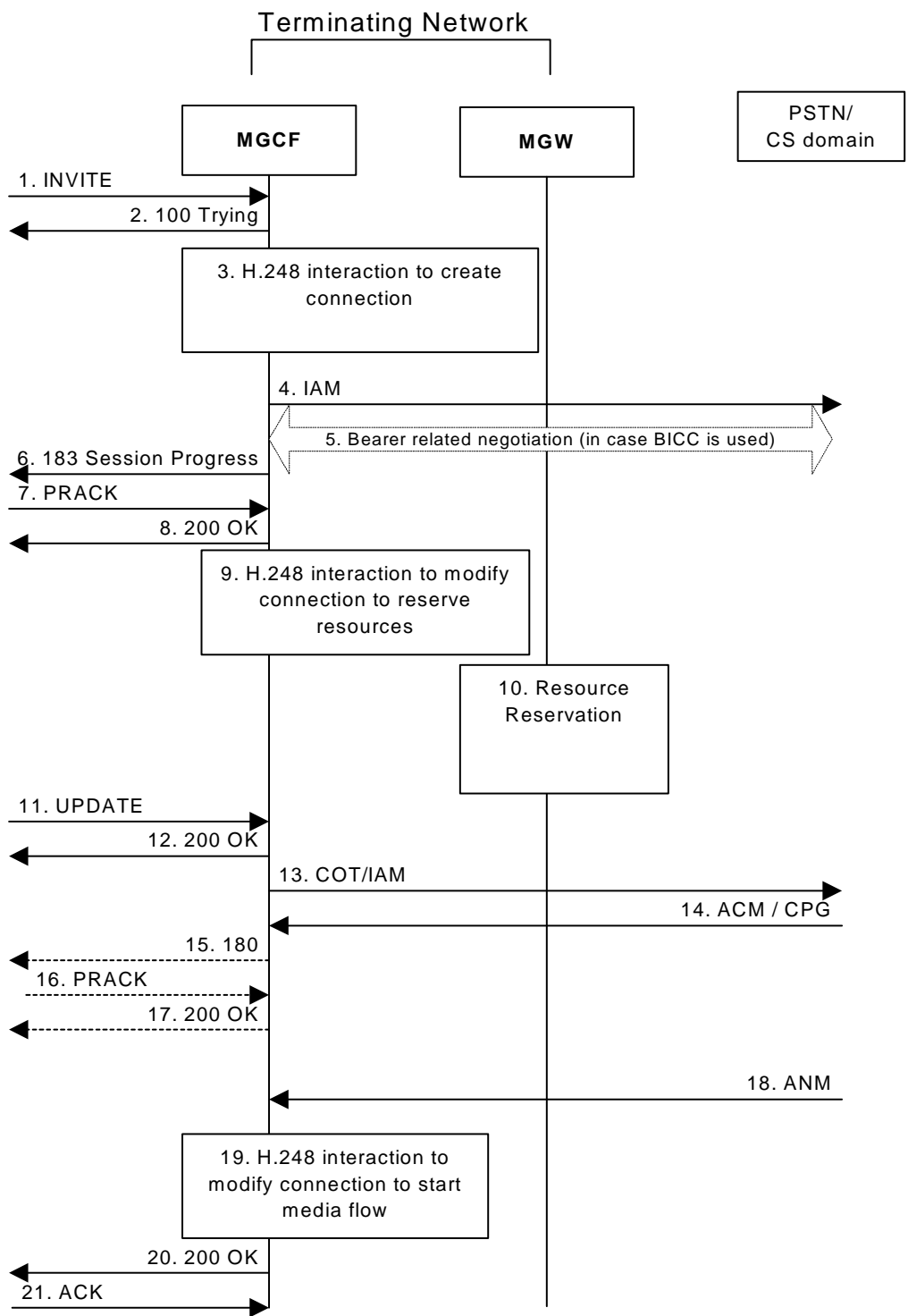


Figure 7.4.4.1-1: CS Networks termination

The CS Networks termination procedure is as follows:

1. INVITE (S-S to CS-T) – see example in table 7.4.4.1-1

MGCF receives an INVITE request, through one of the origination procedures and via one of the S-CSCF to S-CSCF procedures.

Table 7.4.4.1-1: INVITE (S-S to CS-T)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
    ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

P-Charging-Vector: The S-CSCF passes this header to the MGCF for charging. If S-CSCF and MGCF are in different networks (S-S#4), then orig-ioi is included here and the term-ioi would be included in the 183 response.

P-Charging-Function-Addresses: The S-CSCF inserts this header to provide the charging function addresses to the MGCF if S-CSCF and MGCF are in the same network (S-S#3). This header is not present when S-CSCF and MGCF are in different networks (S-S#4).

Upon receiving the INVITE, the MGCF stores the following information about this session – see example in table 7.4.4.1-1b.

Table 7.4.4.1-1b: Storage of information at MGCF

```

Request-URI: tel:+1-212-555-2222
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 127 INVITE
Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

2. 100 Trying (CS-T to S-S) – see example in table 7.4.4.1-2

MGCF may respond to the INVITE request with a 100 Trying provisional response.

Table 7.4.4.1-2: 100 Trying (CS-T to S-S)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. H.248 Interaction to Create Connection

MGCF initiates a H.248 interaction to pick an outgoing channel and determine media capabilities of the MGW.

4. SS7: IAM

Based on the continuity support of the outgoing channel selected, MGCF may decide to send an IAM message out to the CS Networks at this point. In case the outgoing channel does not support continuity indication, MGCF sends out an IAM message only in step 14.

5. Possible bearer related negotiation takes place (in case BICC is used)

6. 183 Session Progress (CS-T to S-S) – see example in table 7.4.4.1-6

MGCF determines the subset of the media flows proposed by the originating endpoint that it supports, and responds with a 183 Session Progress response back to the originator. This response is sent via the S-CSCF to S-CSCF procedure.

NOTE: in order to be able to send the IAM message at step 4, the MGCF has to select one media from the SDP received in INVITE.

Table 7.4.4.1-6: 183 Session Progress (CS-T to S-S)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP bgcf1.home1.net;branch=z9hG4bK6546q2.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: <tel:+1-212-555-2222>
P-Charging-Vector:
Privacy: none
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:mgcf1.home1.net>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

7. PRACK (S-S to CS-T) – see example in table 7.4.4.1-7

The originating endpoint sends a PRACK request. This request does not contain SDP because there was only one media flow with one codec in the first SDP offer/answer negotiation.

Table 7.4.4.1-7: PRACK (S-S to CS-T)

```

PRACK sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 128 PRACK
RAck: 9021 127 INVITE
Content-Length: 0

```

8. 200 OK (CS-T to S-S) – see example in table 7.4.4.1-8

MGCF acknowledges the PRACK request (8) with a 200 OK response.

Table 7.4.4.1-8: 200 OK (CS-T to S-S)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

9. H.248 Interaction to Modify Connection

MGCF initiates a H.248 interaction to modify the connection established in step #3 and instruct MGW to reserve the resources necessary for the media streams.

10. Resource Reservation

MGW reserved the resources necessary for the media streams.

11. UPDATE (S-S to CS-T) – see example in table 7.4.4.1-11

When the originating endpoint has completed its resource reservation, it sends the UPDATE request to MGCF, via the S-CSCF to S-CSCF procedures.

Table 7.4.4.1-11: UPDATE (S-S to CS-T)

```
UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
```

12. 200 OK (CS-T to S-S) – see example in table 7.4.4.1-12

MGCF acknowledges the UPDATE request (11) with a 200 OK response.

Table 7.4.4.1-12: 200 OK (CS-T to S-S)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 0 RTP/AVP 98 99
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxtime:20

```

Remainder of subclause not shown

PROPOSED CHANGE

7.4.5.1 (MT#1c) Mobile termination, roaming, without I-CSCF in home network providing configuration independence, terminating UE is busy, and not able or not willing to answer the call (MO#2, S-S#2 assumed)

Figure 7.4.5.1 shows a termination procedure which applies to roaming subscribers when the home network operator does not desire to keep its internal configuration hidden from the visited network. The UE is located in a visited network, and determines the P-CSCF via the CSCF discovery procedure. During registration, the home network allocates the S-CSCF.

When registration is complete, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE.

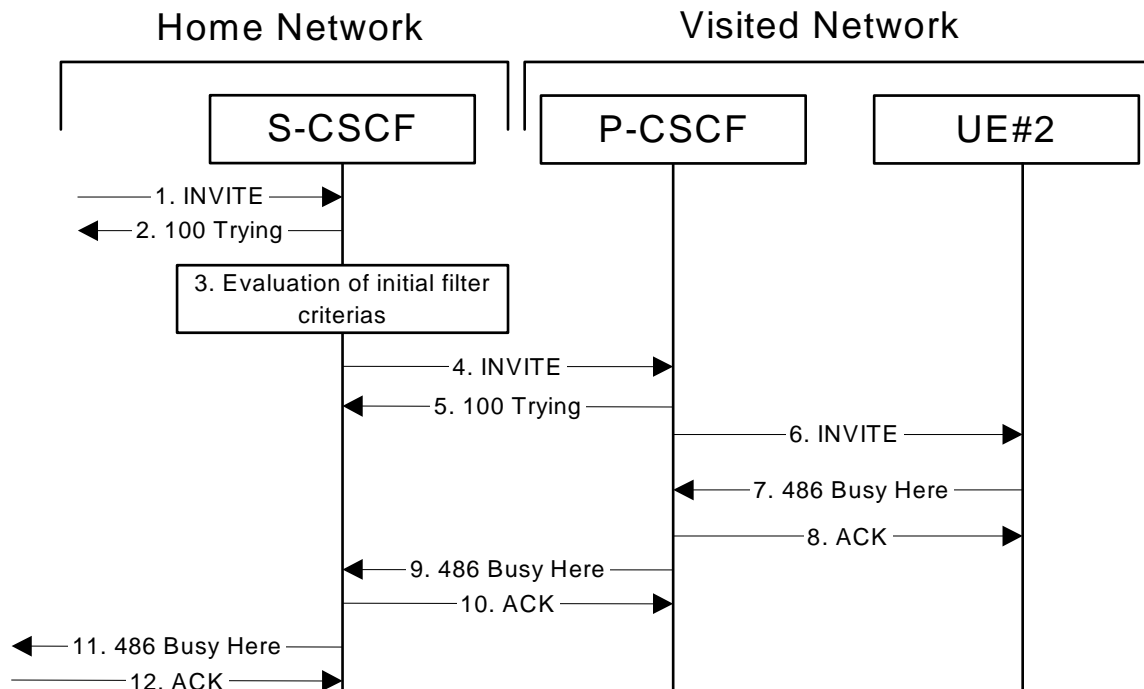


Figure 7.4.5.1-1: MT#1c

Procedure MT#1c is as follows:

1. INVITE (S-S to MT#1a) – see example in table 7.4.5.1-1

The calling party sends the INVITE request, via one of the origination procedures and via one of the S-CSCF to S-CSCF procedures, to the S-CSCF for the terminating subscriber.

Table 7.4.5.1-1: INVITE (S-S to MT#1c)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAfrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtmpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtmpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtmpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtmpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (MT#1c to S-S) – see example in table 7.4.5.1-2

S-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.4.5.1-2: 100 Trying (MT#1c to S-S)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias.

4. INVITE (S-CSCF to P-CSCF) – see example in table 7.4.5.1-4

S-CSCF remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE to the P-CSCF.

Table 7.4.5.1-4: INVITE (S-CSCF to P-CSCF)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Called-Party-ID: Includes the received URI with its parameters

Route: Built from the Path header.

Via:, Record-Route: S-CSCF adds itself

5. 100 Trying (P-CSCF to S-CSCF) – see example in table 7.4.5.1-5

P-CSCF responds to the INVITE request (4) with a 100 Trying provisional response.

Table 7.4.5.1-5: 100 Trying (P-CSCF to S-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

6. INVITE (P-CSCF to UE) – see example in table 7.4.5.1-6

P-CSCF forwards the INVITE request to the UE.

Table 7.4.5.1-6: INVITE (P-CSCF to UE)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
    scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
    <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Media-Authorization:
    0020000100100101706466322e76697369746564322e6e6574000c02013331533134363231
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Media-Authorization: A P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf2.visited2.net" with credentials "31S14621".

Record-Route: The P-CSCF adds the port number negotiated in the security agreement and the comp=sigcomp parameter to its own SIP URI.

Remainder of subclause not shown

PROPOSED CHANGE

7.4.7.1 (MT#1e) Mobile termination, roaming, without I-CSCF in home network providing configuration independence, service is refused by S-CSCF when receiving INVITE request (MO#2, S-S#2 assumed)

Figure 7.4.7.1-1 shows a termination procedure, which applies to roaming subscribers when the home network operator does not desire to keep its internal configuration hidden from the visited network. The UE is located in a visited network, and determines the P-CSCF via the CSCF discovery procedure. During registration, the home network allocates the S-CSCF.

When registration is complete, S-CSCF knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE.

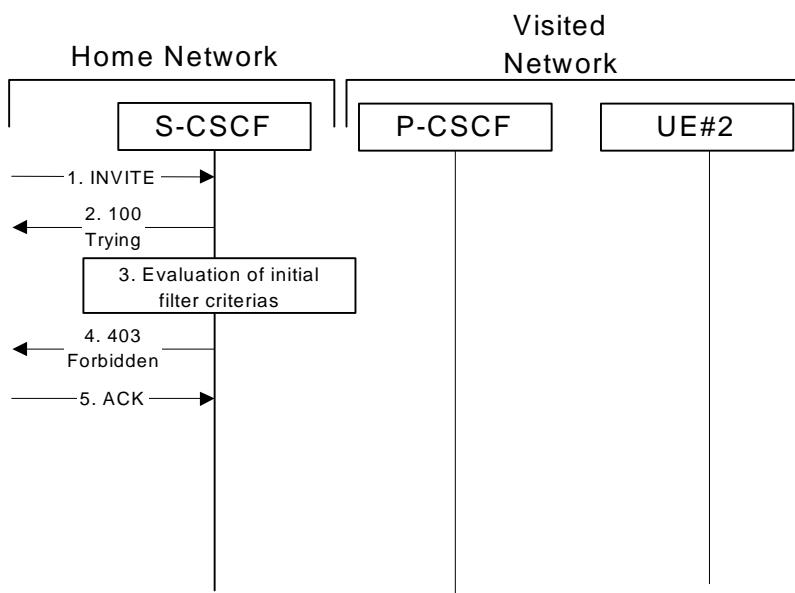


Figure 7.4.7.1-1: Mobile termination, roaming, without I-CSCF in home network providing configuration independence, service is refused by S-CSCF when receiving INVITE request

1. INVITE (S-S to MT#1e) - see example in table 7.4.7.1-1

The calling party sends the INVITE request, via one of the origination procedures and via one of the S-CSCF to S-CSCF procedures, to the S-CSCF for the terminating subscriber.

Table 7.4.7.1-1: INVITE (S-S to MT#1e)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

Remainder of subclause not shown

PROPOSED CHANGE

7.4.9.2 Mobile termination, unregistered subscriber, no services related to unregistered state

In the example information flow the subscriber is unregistered and the subscriber has no services related to unregistered state. This is shown in the following information flow (figure 7.4.9.2-1).

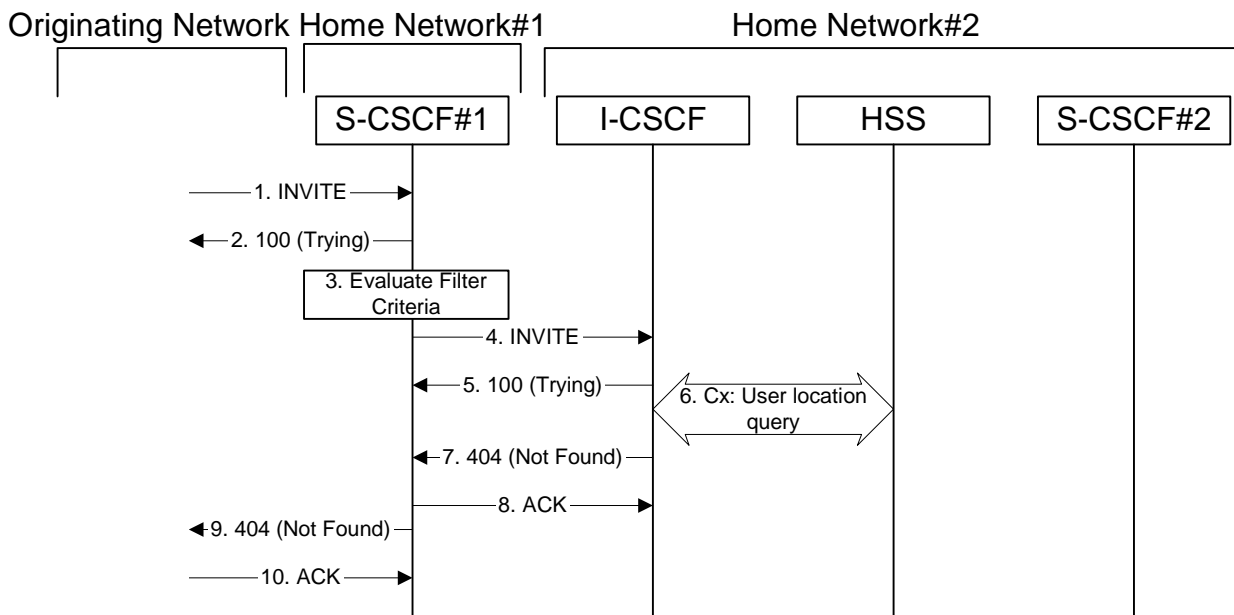


Figure 7.4.9.2-1: Mobile termination, unregistered subscriber

1. INVITE (MO to S-S#1a) – see example in table 7.4.9.2-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 7.4.9.2-1: INVITE (MO to S-S#1a)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:99 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
    
```

2. 100 Trying (S-S#1a to MO) – see example in table 7.4.9.2-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.4.9.2-2: 100 Trying (S-S#1a to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
    
```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias.

For this example, assume no Application Server involvement.

4. INVITE (S-CSCF to I-CSCF) – see example in table 7.4.9.2-4

S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since the originating operator does not desire to keep their internal configuration hidden, S-CSCF#1 forwards the INVITE request directly to I-CSCF in the destination network.

As the S-CSCF does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

Table 7.4.9.2-4: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Remainder of subclause not shown

PROPOSED CHANGE

7.4.9.3 Mobile termination, unregistered subscriber, services related to unregistered state

In the example information flow the subscriber is unregistered and the subscriber has services related to unregistered state. This is shown in the following information flow (figure 7.4.9.3-1).

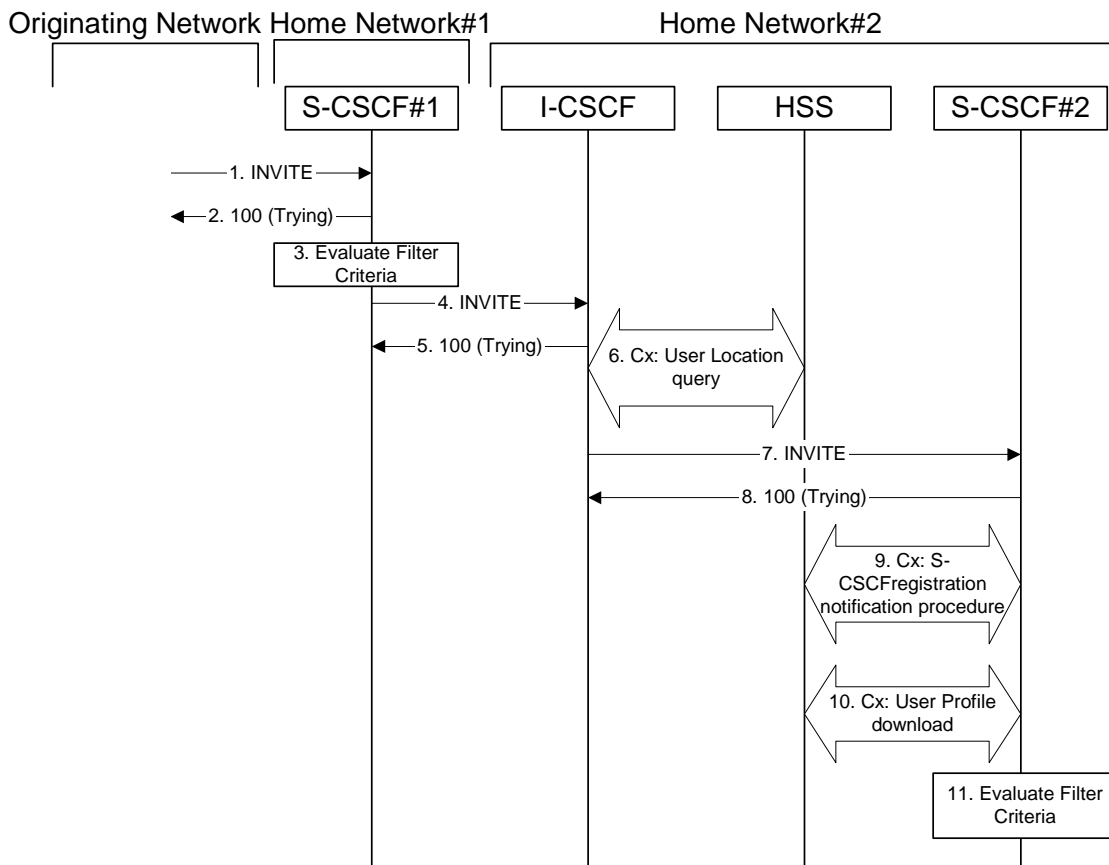


Figure 7.4.9.3-1: Mobile termination, unregistered subscriber with services

1. INVITE (MO to S-S#1a) – see example in table 7.4.9.3-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 7.4.9.3-1: INVITE (MO to S-S#1a)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=ftmp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmt:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (S-S#1a to MO) – see example in table 7.4.9.3-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 7.4.9.3-2: 100 Trying (S-S#1a to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias.

For this example, assume no Application Server involvement.

4. INVITE (S-CSCF to I-CSCF) – see example in table 7.4.9.3-4

S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since the originating operator does not desire to keep their

internal configuration hidden, S-CSCF#1 forwards the INVITE request directly to to I-CSCF in the destination network.

As the S-CSCF does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

Table 7.4.9.3-4: INVITE (S-CSCF to I-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

5. 100 Trying (I-CSCF to S-CSCF) – see example in table 7.4.9.3-5

I-CSCF responds to the INVITE request (4) by sending a 100 Trying provisional response to S-CSCF#1.

Table 7.4.9.3-5: 100 Trying (I-CSCF to S-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

6. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the information that the user is not currently registered, but the user has services when the user is not registered.

For detailed message flows see 3GPP TS 29.228.

Table 7.3.2.1-6a provides the parameters in the SIP INVITE request (flow 4), which are sent to the HSS.

Based on the CX response the I-CSCF selects an appropriate S-CSCF.

7. INVITE (I-CSCF to S-CSCF) – see example in table 7.4.9.3-7

The I-CSCF forwards the REGISTER request to the S-CSCF selected.

Table 7.4.9.3-7: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
      scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
      pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7)
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Allow:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Remainder of subclause not shown

PROPOSED CHANGE

- 7.5.3 Session attempt rejected by the network due to unauthorized media parameters

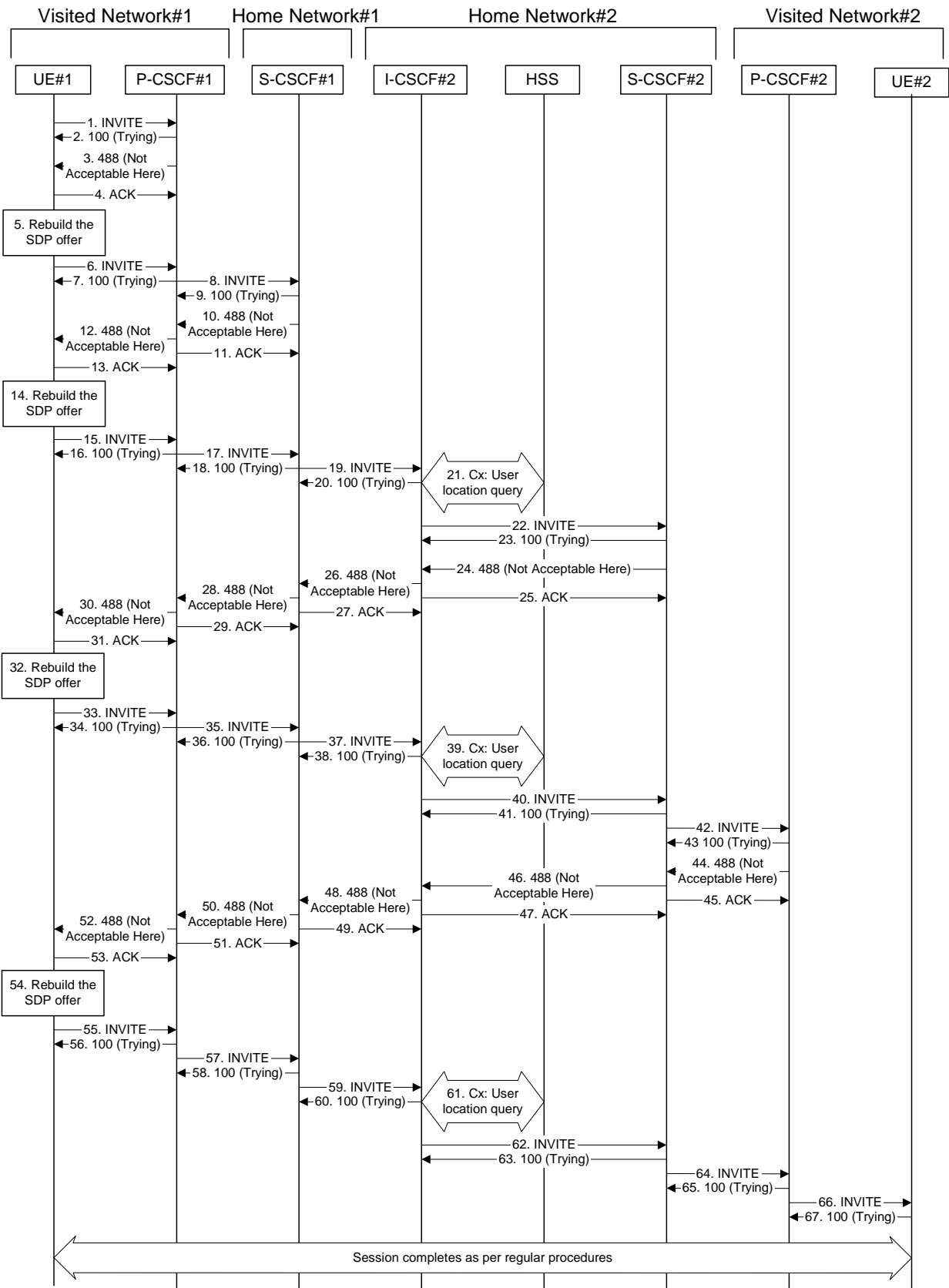


Figure 7.5.3-1: Session rejected by the network due to unauthorized media parameters

Figure 7.5.3-1 shows an example of how the network entities, such as the P-CSCF or the S-CSCF can reject a session attempt due to unauthorized media parameters.

This example shows the worst case scenario, where both P-CSCFs (originating and terminating) and both S-CSCFs (originating and terminating) involved in the session setup reject some part of the media.

For this example, we assume that the UE initiates the session attempt requiring a relatively large amount of media streams and codecs.

1. INVITE (UE1 to P-CSCF1) - see example in table 7.5.3-1

The UE sends the INVITE request, containing an initial SDP, to the P-CSCF1. The initial SDP offer includes three media streams: video, audio and whiteboard. Each media stream contains support for several codecs.

Table 7.5.3-1: INVITE (UE to P-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
  port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99 31 32
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
a=rtpmap:31 H261/90000
a=rtpmap:32 MPV/90000
m=audio 3456 RTP/AVP 97 0 8 100 96
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:100 iLBC
a=rtpmap:96 telephone-event
a=maxptime:20
m=application 32416 udp wb
b=AS:10
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv

```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

2. 100 Trying (P-CSCF1 to UE1) - No example provided

3. 488 Not Acceptable Here (P-CSCF1 to UE1) – see example in table 7.5.3-3

The P-CSCF inspects the media parameters in the SDP offer, and finds that, according to the local policy in the network, users are not allowed to use G.711 audio codecs (payload types 0 and 8 in the SDP audio media stream line). Therefore the P-CSCF1 builds a 488 (Not Acceptable Here) response that includes all the media parameters supported by the visited network in the SDP.

This SDP does not constitute an answer, because it is sent in a non 100-class or 200-class response. This SDP contains the list of media parameters allows by the visited network according to the local policy.

Table 7.5.3-3: 488 Not Acceptable Here (P-CSCF1 to UE1)

```
SIP/2.0 488 Not Acceptable Here
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=223432
Call-ID: cb03a0s09a2sdfglkj490333
CSeq: 127 INVITE
Content-Type: application/sdp
Warning: 305 pcscf1.visited1.net "Incompatible media format"
Content-Length: (...)

v=0
o=- 3087933623 3087933623 IN IP6 pcscf1.visited1.net
s=-
c=IN IP6 pcscf1.visited1.net
t=0 0
m=video 0 RTP/AVP 98 99 26
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=fmtp:98 profile-level-id=0
a=rtpmap:26 JPEG/90000
m=audio 0 RTP/AVP 97 2 3 100 96
a=rtpmap:97 AMR
a=rtpmap:100 iLBC
a=rtpmap:2 G721/8000
a=rtpmap:3 GSM/8000
a=rtpmap:96 telephone-event
a=maxptime:20
m=application 0 udp wb
```

4. ACK (UE1 to P-CSCF1) – see example in table 7.3.5-4

The UE sends an ACK request to the 488 (Not Acceptable Here) response.

Table 7.3.5-4: ACK (UE1 to P-CSCF1)

```
ACK sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
From:
To:
Call-ID:
Cseq: 127 ACK
Content-Length: 0
```

5. Rebuild the SDP offer

Based on the SDP received in the 488 (Not Acceptable Here) response (4), and based on the initial SDP sent in the INVITE request (1), the UE creates a new SDP offer that does not contain the G711 codecs not allowed by pcscf1.visited.net.

6. INVITE (UE1 to P-CSCF1) - see example in table 7.5.3-6

The UE sends the INVITE request, containing an SDP offer, to the P-CSCF1. This SDP offer is based on the initial SDP offer, but it does not contain the G711 codecs.

Table 7.5.3-6: INVITE (UE to P-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 128 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
    port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99 31 32
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
a=rtpmap:31 H261/90000
a=rtpmap:32 MPV/90000
m=audio 3456 RTP/AVP 97 100 96
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:100 iLBC
a=rtpmap:96 telephone-event
a=maxptime:20
m=application 32416 udp wb
b=AS:10
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv

```

7-9. 100 Trying (P-CSCF1 to UE) et seq.

The session continues as per normal procedures.

10. 488 Not Acceptable Here (S-CSCF1 to P-CSCF1) - see example in table 7.5.3-10

The S-CSCF1 inspects the media parameters in the SDP offer, and finds that, according to the local policy or subscription, the subscriber is not allowed to use the whiteboard media stream. Therefore the S-CSCF1 builds a 488 (Not Acceptable Here) response that includes all the media parameters supported by the local policy and the subscriber policy. This SDP does not include the whiteboard media stream.

This SDP does not constitute an answer, because it is sent in a non 100-class or 200-class response. This SDP contains the list of media parameters allows by the originating home network according to the local policy and the originating subscriber policy.

Table 7.5.3-10: 488 Not Acceptable Here (S-CSCF1 to P-CSCF1)

```

SIP/2.0 488 Not Acceptable Here
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKKnashds7
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=223432
Call-ID: cb03a0s09a2sdfgklkj490333
CSeq: 127 INVITE
Content-Type: application/sdp
Warning: 304 scscf1.home1.net "Media type not available"
Content-Length: (...)

v=0
o=- 4087933666 4087933666 IN IP6 scscf1.home1.net
s=-
c=IN IP6 scscf1.home1.net
t=0 0
m=video 0 RTP/AVP 98 99 26
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=rtpmap:26 JPEG/90000
m=audio 0 RTP/AVP 97 2 3 9 100 0 8 96
a=rtpmap:97 AMR
a=rtpmap:2 G721/8000
a=rtpmap:3 GSM/8000
a=rtpmap:9 G722/8000
a=rtpmap:100 iLBC
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event

```

11-13. ACK (S-CSCF1 to P-CSCF1) et seq.

The session continues as per normal procedures.

14. Rebuild the SDP offer

Based on the SDP received in the 488 (Not Acceptable Here) response (12), and based on the SDP sent in the INVITE request (6), the UE creates a new SDP offer that does not contain the whiteboard media stream not allowed by scscf1.home1.net.

15. INVITE (UE1 to P-CSCF1) - see example in table 7.5.3-15

The UE sends the INVITE request, containing an SDP offer, to the P-CSCF determined via the CSCF discovery mechanism. This SDP offer is based on the previous SDP offer, but it does not contain the whiteboard media streams.

Table 7.5.3-15: INVITE (UE to P-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 129 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
    port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99 31 32
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
a=rtpmap:31 H261/90000
a=rtpmap:32 MPV/90000
m=audio 3456 RTP/AVP 97 100 96
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:100 iLBC
a=rtpmap:96 telephone-event
a=maxptime:20

```

16-23. 100 Trying (P-CSCF1 to UE) et seq.

The session continues as per normal procedures,

24. 488 Not Acceptable Here (S-CSCF2 to I-CSCF2) - see example in table 7.5.3-24

The S-CSCF2 inspects the media parameters in the SDP offer, and finds that, according to the local policy or the terminating user subscription, the user is not allowed to use the video media stream. Therefore the S-CSCF1 builds a 488 (Not Acceptable Here) response that includes all the media parameters supported by the local policy and the subscriber policy. This SDP does not include the video media stream.

This SDP does not constitute an answer, because it is sent in a non 100-class or 200-class response. This SDP contains the list of media parameters allowed by the terminating home network according to the local policy and the terminating subscriber policy.

Table 7.5.3-24: 488 Not Acceptable Here (S-CSCF2 to I-CSCF2)

```

SIP/2.0 488 Not Acceptable Here
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=678358
Call-ID: cb03a0s09a2sdfglkj490333
CSeq: 127 INVITE
Content-Type: application/sdp
Warning: 304 scscf2.home1.net "Media type not available"
Content-Length: (...)

v=0
o=- 561363252345 561363252345 IN IP6 scscf2.home2.net
s=-
c=IN IP6 scscf2.home2.net
t=0 0
m=audio 0 RTP/AVP 97 2 3 9 100 96
a=rtpmap:97 AMR
a=rtpmap:2 G721/8000
a=rtpmap:3 GSM/8000
a=rtpmap:9 G722/8000
a=rtpmap:100 iLBC
a=rtpmap:96 telephone-event
m=application 0 udp wb

```

25-31. ACK (I-CSCF2 to S-CSCF2) et seq.

The session continues as per normal procedures.

32. Rebuild the SDP offer

Based on the SDP received in the 488 (Not Acceptable Here) response (24), and based on the SDP sent in the INVITE request (15), the UE creates a new SDP offer that does not contain the whiteboard media stream not allowed by scscf2.home2.net.

33. INVITE (UE1 to P-CSCF1) - see example in table 7.5.3-33

The UE sends the INVITE request, containing an SDP offer, to the P-CSCF1. This SDP offer is based on the previous SDP offer, but it does not contain the video media stream.

Table 7.5.3-33: INVITE (UE to P-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=667788
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 130 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
    port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933618 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 100 96
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:100 iLBC
a=rtpmap:96 telephone-event
a=maxptime:20

```

34-43. 100 Trying (P-CSCF1 to UE) et seq.

The session continues as per normal procedures,

44. 488 Not Acceptable Here (P-CSCF2 to S-CSCF2) - see example in table 7.5.3-44

The P-CSCF2 inspects the media parameters in the SDP offer, and finds that, according to the local policy, the iLBC codec is not allowed. Therefore the P-CSCF2 builds a 488 (Not Acceptable Here) response that includes all the media parameters supported by the local policy.

This SDP does not constitute an answer, because it is sent in a non 100-class or 200-class response. This SDP contains the list of media parameters allows by the terminating visited network according to the local policy.

Table 7.5.3-44: 488 Not Acceptable Here (S-CSCF2 to I-CSCF2)

```

SIP/2.0 488 Not Acceptable Here
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From: <sip:user1_public1@home1.net>;tag=667788
To: <sip:user2_public1@home2.net>;tag=987654
Call-ID: cb03a0s09a2sdfglkj490333
CSeq: 130 INVITE
Content-Type: application/sdp
Warning: 305 pcscf2.visited2.net "Incompatible media format"
Content-Length: (...)

v=0
o=- 4087933666 4087933666 IN IP6 pcscf2.visited2.net
s=-
c=IN IP6 pcscf2.visited2.net
t=0 0
m=audio 0 RTP/AVP 97 2 3 9 96
a=rtpmap:97 AMR
a=rtpmap:2 G721/8000
a=rtpmap:3 GSM/8000
a=rtpmap:9 G722/8000
a=rtpmap:96 telephone-event
m=application 0 udp wb
m=video 0 RTP/AVP 98 99 26
a=rtpmap:98 H263
a=rtpmap:99 MP4V-ES
a=fmtp:98 profile-level-id=0
a=rtpmap:26 JPEG/90000

```

45-53. ACK (S-CSCF2 to P-CSCF2) et seq.

The session continues as per normal procedures.

54. Rebuild the SDP offer

Based on the SDP received in the 488 (Not Acceptable Here) response (52), and based on the SDP sent in the INVITE request (33), the UE creates a new SDP offer that does not contain the iBLC coded not allowed by pcscf2.visited.net.

55. INVITE (UE1 to P-CSCF1) - see example in table 7.5.3-55

The UE sends the INVITE request, containing an SDP offer, to the P-CSCF1. This SDP offer is based on the previous SDP offer, but it does not contain the video media stream.

Table 7.5.3-55: INVITE (UE to P-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=667788
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 131 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
    port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933619 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=audio 3456 RTP/AVP 97 96
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

Remainder of subclause not shown

PROPOSED CHANGE

10.1.2 Mobile-to-mobile session hold and resume procedures

A session was previously established between an initiating UE and a terminating UE. Each of these UEs has an associated P-CSCF in the same network where they are currently located (either home or roaming), and a S-CSCF assigned in their home network. These functional elements co-operate to clear the session, and the procedures are independent of whether they are located in the home or visited networks.

The hold and resume procedures are identical whether the UE that initiated the session also initiates the session-hold, or whether the UE that terminated the session initiates the session-hold.

When a media stream has been placed on hold, it should not be resumed by any endpoint other than the one that placed it on hold.

These procedures show only one combination of Mobile-Originated, Serving-to-Serving, and Mobile-Terminated procedures, MO#2, S-S#2, and MT#2. These procedures do not show the use of optional I-CSCFs. If an I-CSCF was included in the signalling path during the session establishment procedure, it would continue to be used in any subsequent signalling flows such as the ones described in this clause. Procedures at the I-CSCFs are identical to those described for the BYE, PRACK, and UPDATE requests and responses described in other clauses.

As this flow does not require a user interaction at the remote end, it is realized with an UPDATE request.

The procedures for placing a media stream on hold, and later resuming the media stream, are as shown in figure 10.1.2-1:

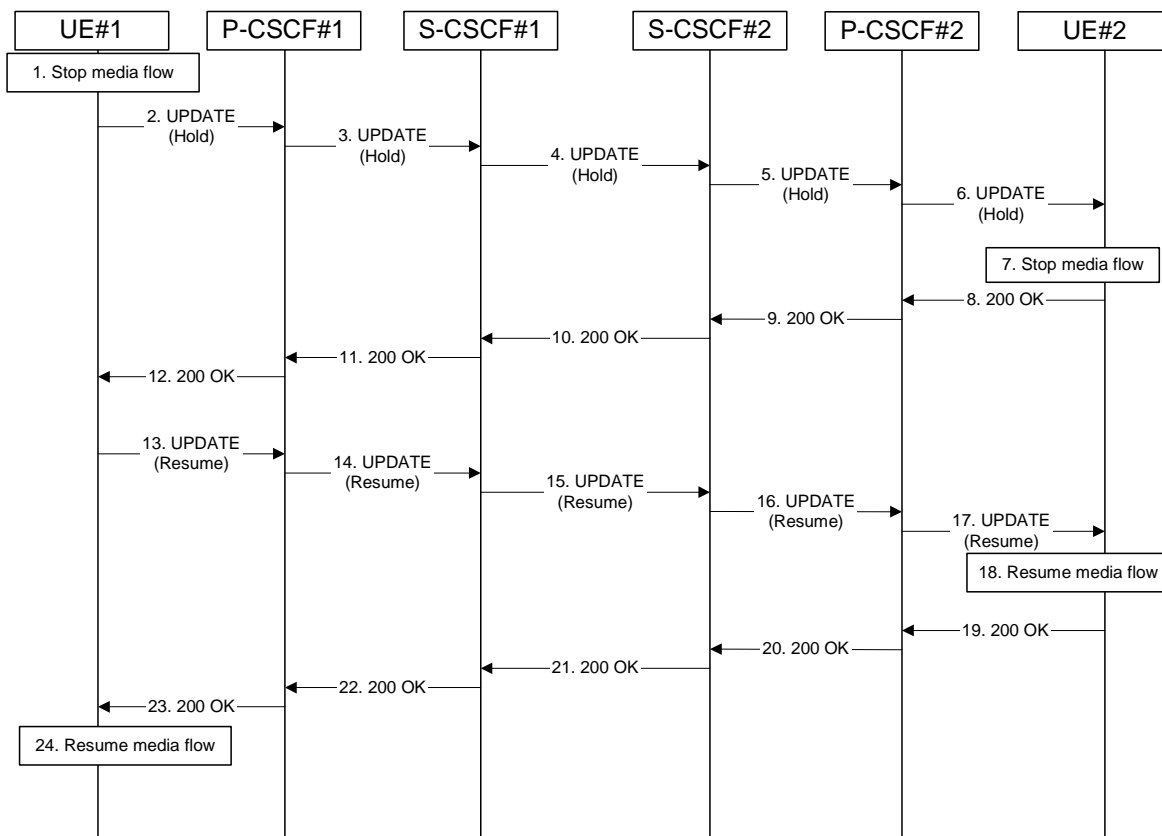


Figure 10.1.2-1: Mobile to mobile session hold and resume

Signalling flow procedures are as follows:

1. Stop Media Flow

UE#1 detects a request from the subscriber to place a media stream on hold. UE#1 stops sending the media stream to the remote endpoint, but keeps the resources for the session reserved.

2. UPDATE(Hold) (UE to P-CSCF) – see example in table 10.1.2-2

UE#1 sends a Hold request to its proxy, P-CSCF#1.

Table 10.1.2-2: UPDATE(Hold) (UE to P-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
<sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 130 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0_0
m=audio 3456 RTP/AVP 97
b=AS:25.4
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
    
```

- Request-URI:** Contains the value of the Contact header from the 200 (OK) response to the initial INVITE.
- Via:** Contains the IP address or FQDN of the originating UE.
- P-Access-Network-Info:** the UE provides the access-type and access-info, related to the serving access network.
- From:/To:/Call-ID:** Contain the values previously used to establish the session, including the tag value from the response.
- Cseq:** Next higher sequential value.
- Security-Verify:** Contains the security agreement as represented by the received Security-Server header.
- SDP** The sendrecv media stream is placed on hold by changing it to inactive media stream, and no media is sent to the far end.

3. UPDATE (Hold) (P-CSCF to S-CSCF) – see example in table 10.1.2-3

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

The P-CSCF#1 forwards the Hold request to S-CSCF#1.

Table 10.1.2-3: UPDATE(Hold) (P-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-forwards: 69
P-Access-Network-Info:
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=

```

P-Access-Network-Info: This header contains information from the UE.

P-Charging-Vector: The P-CSCF inserts this header and populates the icid parameters with a globally unique value.

4. UPDATE(Hold) (S-CSCF to S-CSCF) – see example in table 10.1.2-4

S-CSCF#1 forwards the Hold request to S-CSCF#2.

Table 10.1.2-4: UPDATE(Hold) (S-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=

```

P-Charging-Vector: If the two S-CSCF entities are located in different networks, then the orig-ioi parameter would be included (not shown).

5. UPDATE(Hold) (S-CSCF to P-CSCF) – see example in table 10.1.2-5

S-CSCF#2 forwards the Hold request to P-CSCF#2.

Table 10.1.2-5: UPDATE(Hold) (S-CSCF to P-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-forwards: 67
Route: <sip:pcscf2.home2.net;lr>
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

6. UPDATE(Hold) (P-CSCF to UE) – see example in table 10.1.2-6

P-CSCF#2 forwards the Hold request to UE#2.

Table 10.1.2-6: UPDATE(Hold) (P-CSCF to UE)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK556g98.5, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-forwards: 66
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

Via: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its Via header.

7. Stop Media flow

UE#2 stops sending the media stream to the remote endpoint, but keeps the resources for the session reserved.

8. 200-OK (UE to P-CSCF) – see example in table 10.1.2-8

UE#2 acknowledges receipt of the Hold request (6) with a 200 (OK) final response, sent to P-CSCF#2.

Table 10.1.2-8: 200 OK (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK556g98.5, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0
m=audio 6402 RTP/AVP 97
b=AS:25.4
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

SDP: Since the media stream was offered as inactive, it is marked as inactive in the response.

9. 200-OK (P-CSCF to S-CSCF) – see example in table 10.1.2-9

P-CSCF#2 forwards the 200 OK final response to S-CSCF#2.

Table 10.1.2-9: 200 OK (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
```

P-Access-Network-Info: This header contains information from the UE.

10. 200-OK (S-CSCF to S-CSCF) – see example in table 10.1.2-10

S-CSCF#2 forwards the 200 OK final response to S-CSCF#1.

Table 10.1.2-10: 200 OK (S-CSCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

11. 200-OK (S-CSCF to P-CSCF) – see example in table 10.1.2-11

S-CSCF#1 forwards the 200 OK final response to P-CSCF#1.

Table 10.1.2-11: 200 OK (S-CSCF to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

12. 200-OK (P-CSCF to UE) – see example in table 10.1.2-12

P-CSCF#1 forwards the 200 OK final response to UE#1.

Table 10.1.2-12: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
```

13. UPDATE(Resume) (UE to P-CSCF) – see example in table 10.1.2-13

UE#1 detects a request from the subscriber to resume the media stream previously placed on hold.
UE#1 sends a Resume request to its proxy, P-CSCF#1.

Table 10.1.2-13: UPDATE(Resume) (UE to P-CSCF)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
<sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 131 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275-0 0
m=audio 3456 RTP/AVP 97
b=AS:25.4
a=sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

- Request-URI:** Contains the value of the Contact header from the 200 (OK) response to the initial INVITE.
- Via:** Contains the IP address or FQDN of the originating UE.
- From:/To:/Call-ID:** Contain the values previously used to establish the session, including the tag value from the response.
- Cseq:** Next higher sequential value.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

SDP: Same SDP as negotiated during the session setup, restores the sendrecv media stream.

14. UPDATE(Resume) (P-CSCF to S-CSCF) – see example in table 10.1.2-14

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

The P-CSCF#1 forwards the Resume request to S-CSCF#1.

Table 10.1.2-14: UPDATE(Resume) (P-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-forwards: 69
P-Access-Network-Info:
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

P-Charging-Vector: The P-CSCF inserts this header and populates the icid parameters with a globally unique value.

15. UPDATE(Resume) (S-CSCF to S-CSCF) – see example in table 10.1.2-15

S-CSCF#1 forwards the Resume request to S-CSCF#2.

Table 10.1.2-15: UPDATE(Resume) (S-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=

```

16. UPDATE(Resume) (S-CSCF to P-CSCF) – see example in table 10.1.2-16

S-CSCF#2 forwards the Resume request to P-CSCF#2.

Table 10.1.2-16: UPDATE(Resume) (S-CSCF to P-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
  scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-forwards: 67
Route: <sip:pcscf2.home2.net;lr>
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=

```

17. UPDATE(Resume) (P-CSCF to UE) – see example in table 10.1.2-17

P-CSCF#2 forwards the Resume request to UE#2.

Table 10.1.2-17: UPDATE(Resume) (P-CSCF to UE)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK556g98.5, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-forwards: 66
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=

```

Via: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its Via header.

18. Resume media flow

UE#2 resumes sending the media stream to the remote endpoint.

19. 200-OK (UE to P-CSCF) – see example in table 10.1.2-19

UE#2 acknowledges receipt of the Resume request (17) with a 200 (OK) final response, sent to P-CSCF#2.

Table 10.1.2-19: 200 OK (UE to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK556g98.5, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275-0 0
m=audio 6402 RTP/AVP 97
b=AS:25.4
a=sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

20. 200-OK (P-CSCF to S-CSCF) – see example in table 10.1.2-20

P-CSCF#2 forwards the 200 OK final response to S-CSCF#2.

Table 10.1.2-20: 200 OK (P-CSCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

21. 200-OK (S-CSCF to S-CSCF) – see example in table 10.1.2-21

S-CSCF#2 forwards the 200 OK final response to S-CSCF#1.

Table 10.1.2-21: 200 OK (S-CSCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

22. 200-OK (S-CSCF to P-CSCF) – see example in table 10.1.2-22

S-CSCF#1 forwards the 200 OK final response to P-CSCF#1.

Table 10.1.2-22: 200 OK (S-CSCF to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

23. 200-OK (P-CSCF to UE) – see example in table 10.1.2-23

P-CSCF#1 forwards the 200 OK final response to UE#1.

Table 10.1.2-23: 200 OK (P-CSCF to UE)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

24. UE Resume Media Flow

PROPOSED CHANGE

10.1.3 Mobile-initiated hold and resume of a mobile-PSTN session

An IM session was previously established between an initiating UE and a MGCF acting as a gateway for a session terminating on the PSTN, or between an initiating MGCF acting as a gateway for a session originating on the PSTN to a terminating UE. The UE has an associated P-CSCF in the same network where it is currently located (either home or roaming), an S-CSCF assigned in its home network, and a BGCF that chooses the MGCF. These functional elements co-operate to clear the session, and the procedures are independent of whether they are located in the subscriber's home or visited networks. Therefore there is no distinction in this clause of home network vs. visited network.

The session hold and resume procedure is similar whether the UE initiated the session to the PSTN, or if the PSTN initiated the session to the UE. The only difference is the optional presence of the BGCF in the case of a session initiated by the UE. The BGCF might or might not be present in the signalling path after the first INVITE is routed.

These procedures show only one combination of Mobile-Originated, Serving-to-Serving, and Mobile-Terminated procedures, MO#2, S-S#3, and CS-T. These procedures do not show the use of optional I-CSCFs, or the use of the BGCF in achieving network configuration independence. If an I-CSCF/BGCF was included in the signalling path during the session establishment procedure, it would continue to be used in any subsequent signalling flows such as the ones described in this clause. Procedures at the I-CSCFs are identical to those described for the BYE, PRACK, and UPDATE requests and responses described in other clauses.

As this flow does not require a user interaction at the remote end, it is realized with an UPDATE request.

The procedures for placing a media stream on hold, and later resuming the media stream, are as shown in figure 10.1.3-1:

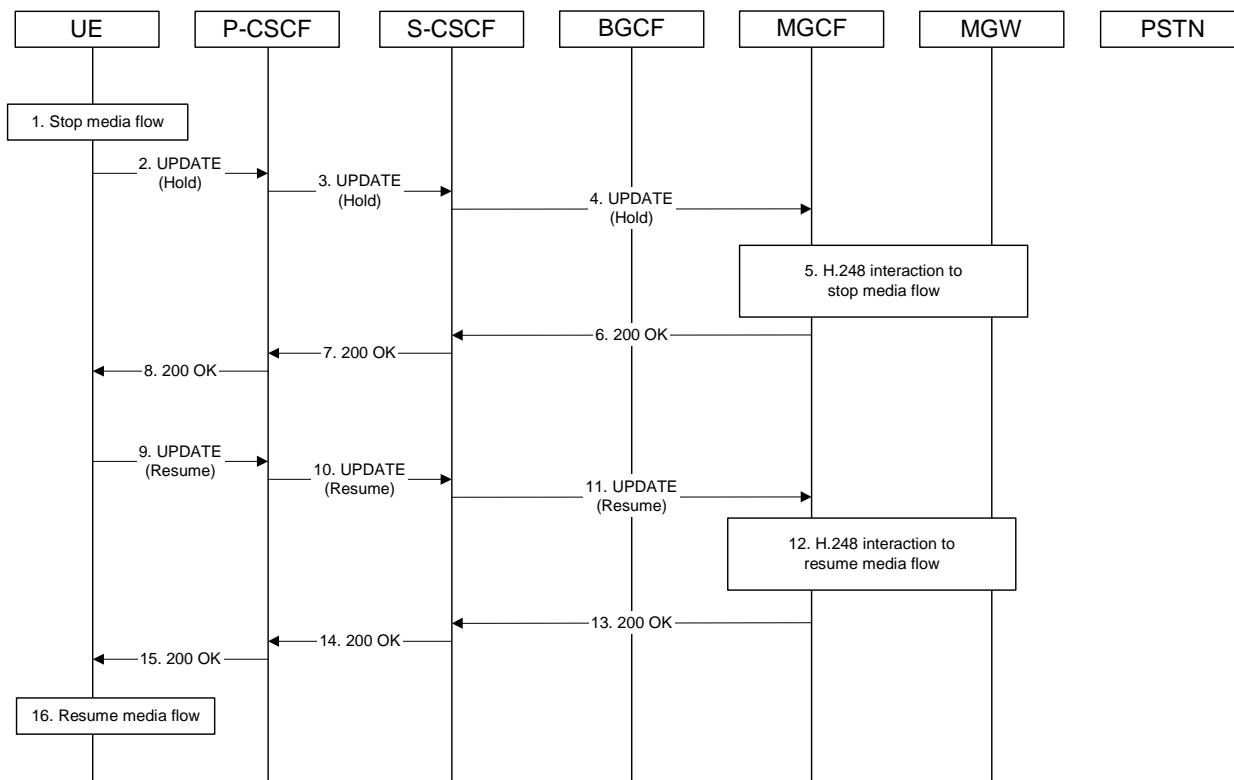


Figure 10.1.3-1: Mobile to PSTN session hold and resume

Signalling flow procedures are as follows:

1. Stop Media Flow

UE#1 detects a request from the subscriber to place a media stream on hold. UE#1 stops sending the media stream to the remote endpoint, but keeps the resources for the session reserved.

2. UPDATE (Hold) (UE to P-CSCF) – see example in 10.1.3-2

UE sends a Hold request to its proxy, P-CSCF.

Table 10.1.3-2: UPDATE (Hold) (UE to P-CSCF)

```

UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 130 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275-0 0
m=audio 3456 RTP/AVP 97
b=AS:25.4
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

- Request-URI:** Contains the value of the Contact header from the 200 (OK) response to the initial INVITE.
- Via:** Contains the IP address or FQDN of the originating UE.
- P-Access-Network-Info:** the UE provides the access-type and access-info, related to the serving access network.
- From:/To:/Call-ID:** Contain the values previously used to establish the session, including the tag value from the response.
- Cseq:** Next higher sequential value.
- Security-Verify:** Contains the security agreement as represented by the received Security-Server header.
- SDP** The sendrecv media stream is placed on hold by changing it to inactive media stream, and no media is sent to the far end.

3. UPDATE (Hold) (P-CSCF to S-CSCF) – see example in table 10.1.3-3

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

The P-CSCF forwards the Hold request to S-CSCF.

Table 10.1.3-3: UPDATE (Hold) (P-CSCF to S-CSCF)

```

UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Route: <sip:scscf1.home1.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

P-Access-Network-Info: This header contains information from the UE.

P-Charging-Vector: The P-CSCF inserts this header and populates the icid parameters with a globally unique value.

4. UPDATE (Hold) (S-CSCF to MGCF) – see example in table 10.1.3-4

S-CSCF forwards the Hold request to MGCF.

Table 10.1.3-4: UPDATE (Hold) (S-CSCF to MGCF)

```

UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

5. H.248 Interaction to Stop Media flow

MGCF initiates a H.248 interaction with MGW instructing it to stop sending the media stream, but to keep the resources for the session reserved.

6. 200-OK (MGCF to S-CSCF) – see example in table 10.1.3-6

MGCF acknowledges receipt of the Hold request (4) with a 200 (OK) final response, sent to S-CSCF.

Table 10.1.3-6: 200 OK (MGCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0_0
m=audio 3456 RTP/AVP 97
b=AS:25.4
a=inactive
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

SDP: Since the media stream was offered as inactive, it is marked as inactive in the response.

7. 200-OK (S-CSCF to P-CSCF) – see example in table 10.1.3-7

S-CSCF forwards the 200 OK final response to P-CSCF.

Table 10.1.3-7: 200 OK (S-CSCF to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

8. 200-OK (P-CSCF to UE) – see example in table 10.1.3-8

P-CSCF forwards the 200 OK final response to UE.

Table 10.1.3-8: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
```

9. UPDATE (Resume) (UE to P-CSCF) – see example in table 10.1.3-9

UE detects a request from the subscriber to resume the media stream previously placed on hold. UE sends a Resume request to its proxy, P-CSCF.

Table 10.1.3-9: UPDATE (Resume) (UE to P-CSCF)

```
UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.home1.net;lr>, <sip:scscf1.home1.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 131 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275-0 0
m=audio 3456 RTP/AVP 97
b=AS:25.4
a=sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
```

- Request-URI:** Contains the value of the Contact header from the 200 (OK) response to the initial INVITE.
- Via:** Contains the IP address or FQDN of the originating UE.
- From:/To:/Call-ID:** Contain the values previously used to establish the session, including the tag value from the response.
- Cseq:** Next higher sequential value.
- Security-Verify:** Contains the security agreement as represented by the received Security-Server header.

SDP Same SDP as negotiated during the session setup, restores the sendrecv media stream.

10. UPDATE (Resume) (P-CSCF to S-CSCF) – see example in table 10.1.3-10

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

The P-CSCF forwards the Resume request to S-CSCF.

Table 10.1.3-10: UPDATE(Resume) (P-CSCF to S-CSCF)

```

UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Route: <sip:scscf1.home1.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=

```

P-Charging-Vector: The P-CSCF inserts this header and populates the icid parameters with a globally unique value.

11. UPDATE(Resume) (S-CSCF to MGCF) – see example in table 10.1.3-11

S-CSCF forwards the Resume request to MGCF.

Table 10.1.3-11: UPDATE(Resume) (S-CSCF to MGCF)

```

UPDATE sip:mgcf1.home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=

```

12. H.248 Interaction to Resume media flow

MGCF initiates a H.248 interaction with MGW instructing it to resume sending the media stream.

13. 200 OK (MGCF to S-CSCF) – see example in table 10.1.3-13

MGCF acknowledges receipt of the Resume request (11) with a 200 (OK) final response, sent to S-CSCF.

Table 10.1.3-13: 200 OK (MGCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=0
o=- 2987933615 2987933617 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0_0
m=audio 6402 RTP/AVP 97
b=AS:25.4
a=sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

14. 200 OK (S-CSCF to P-CSCF) – see example in table 10.1.3-14

Table 10.1.3-14: 200 OK (S-CSCF to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

15. 200 OK (P-CSCF to UE) – see example in table 10.1.3-15

P-CSCF forwards the 200 OK final response to UE.

Table 10.1.3-15: 200 OK (P-CSCF to UE)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

16. Resume Media Flow

UE resumes sending the media stream to the remote endpoint.

PROPOSED CHANGE

10.2.2 Session originator desiring privacy in asserted identity

If the initiating user desires the session privacy for the asserted identity, the following rules are followed in generating header values:

From:	UE provides an anonymous username.
To:	If a telephone number is used in the addr-spec, the UE provides a tel URL containing a

	full E.164 number including the country code.
Privacy:	UE includes the tag "id"

An example of an initial INVITE request following the rules for a private asserted identity is given in table 10.2.2-1. This revised information would appear as step #1 of MO#1a (subclause 7.2.2), MO#1b (subclause 17.2.2), MO#2 (subclause 7.2.3), and step #4 of CS-O (subclause 7.2.4).

Table 10.2.2-1: INVITE (UE to P-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: id
From: "Anonymous" <sip:anonymous@anonymous.invalid>
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642; port-s=7531
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275-0 0
m=audio 3456 RTP/AVP 97 3 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 G726-32/8000
a=rtpmap:96 telephone-event
a=maxptime:20
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv

```

From: Contains an anonymous SIP URI.

To: Contains the destination TEL URL in international format.

When the destination P-CSCF forwards the INVITE request to the destination UE, it removes the P-Asserted-Identity and Privacy headers. An example is given in table 10.2.2-2

Table 10.2.2-2: INVITE (P-CSCF to UE)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsfc2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k2l.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Record-Route: <sip:pcscf2.visited2.net:5088;comp=sigcomp;lr>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Media-Authorization:
0020000100100101706466312e686f6d65312e6e6574000c02013331533134363231
From:
To:
Call-ID:
Cseq:
Supported:
Require: precondition
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

The UE does not receive a P-Asserted-Identity that can identify the originating of the call.

PROPOSED CHANGE

10.2.3 Session originator without indication of privacy preference

If the initiating user did not state a preference for privacy, local policies and regulations may force the network operator to make the session private for the asserted identity. Therefore, the following rules are followed in generating header values:

From:	UE provides any of the registered public user identities allocated to the user.
To:	If a telephone number is used in the addr-spec, the UE provides a tel URL containing an E.164 number. Otherwise, the UE provides the URI of the destination user.
Privacy:	The UE does not include a Privacy header expressing the user's preferences

An example of an initial INVITE request following the rules for a session that does not include any privacy preferences is given in table 10.2.3-1.

Table 10.2.3-1: INVITE (UE to P-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
port-c=8642; port-s=7531
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0_0
m=audio 3456 RTP/AVP 97 3 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 G726-32/8000
a=rtpmap:96 telephone-event
a=maxptime:20
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv

```

The values of From, To, and P-Asserted-Identity (derived from the P-Preferred-Identity above), as given above, are carried through the INVITE sequence, through the S-CSCF serving the originating subscriber.

Based on local policy or regulatory requirements, the S-CSCF serving the originating subscriber may either allow the identification information to be given to the destination, or may restrict it. In case the originating S-CSCF desires to apply privacy for the P-Asserted-Identity, it introduces a Privacy header value with the "id" tag, as in the example in table 10.2.3-2.

Table 10.2.3-2: INVITE (S-CSCF to S-S)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKdashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
Privacy: id
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
From:
To:
Call-ID:
Cseq:
Require: precondition
Supported:
Contact:
Content-Type:
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0_0
m=video 0 RTP/AVP 99
b=AS:54.6
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:99:MPV
m=video 0 RTP/AVP 99
b=AS:54.6
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:99:MPV
m=audio 3456 RTP/AVP 97 96 0 15
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 G726-32/8000
a=rtpmap:96 telephone-event
a=maxptime:20
m=audio 3458 RTP/AVP 97 96 0 15
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 G726-32/8000
a=rtpmap:96 telephone-event
a=maxptime:20

```

When the destination P-CSCF forwards the INVITE request to the destination UE, the P-CSCF will remove the P-Asserted-Identity. An example is show in table 10.2.2-2.

PROPOSED CHANGE

10.2.4 Session destination desiring privacy in asserted identity

If the destination user desires the P-Asserted-Identity to be private, the UE indicates this in the value of the Privacy header in the first non-100 response to the initial INVITE. An example of this response from UE to P-CSCF (step#8 of MT#1a, step#10 of MT#1b, step#8 of MT#2), is given in table 10.2.4-1.

Table 10.2.4-1: 183 Session Progress (UE to P-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcsf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Record-Route: <sip:pcsf2.home2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Preferred-Identity: "John Smith" <sip:user2_public1@home2.net>
Privacy: id
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=907165275-0 0
m=audio 6544 RTP/AVP 97
b=AS:25.4
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtmpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtmpmap:96 telephone-event
a=maxptime:20
```

P-Preferred-Identity: Provides a hint to identify the answering subscriber. It contains the public user identity, and the name of the answering party.

Privacy: The value "id" is included to indicate that privacy of the asserted identity is requested.

The value of the P-Asserted-Identity header, typically derived from the P-Preferred-Identity header is carried through the 183-Session-Progress sequence, to the originating P-CSCF. When the originating P-CSCF forwards the request to the originating UE, the P-CSCF removes the P-Asserted-Identity and the Privacy headers.

Table 10.2.4-2: 183 Session Progress (P-CSCF to UE)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Media-Authorization:
    0020000100100101706466322e76697369746564322e6e6574000c020139425633303732
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

PROPOSED CHANGE

10.2.5 Session destination without indication of privacy preference

If the destination user did not state a preference for privacy, local policies and regulations may force the network operator to make the session privacy for the asserted identity. The destination UE indicates its lack of preference by not providing a Privacy header. An example of this response from UE to P-CSCF (step#8 of MT#1a, step#10 of MT#1b, step#8 of MT#2), is given in table 10.2.5-1.

Table 10.2.5-1: 183 Session Progress (UE to P-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Preferred-Identity: "John Smith" <sip:user2_public1@home2.net>
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=907165275-0 0
m=audio 6544 RTP/AVP 97
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv'
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

P-Preferred-Identity: Provides a hint to identify the answering subscriber. It contains the public user identity, and the name of the answering party.

Based on local policy or regulatory requirements, the S-CSCF serving the destination subscriber may either allow the identification information to be given to the initiator, or may restrict it (by following the example in subclause 10.2.4-2).

PROPOSED CHANGE

10.4.2 Session redirection initiated by S-CSCF to IM CN subsystem (MO#2, MT#2 assumed)

One of the entities in a basic session that may initiate a redirection is the S-CSCF of the destination subscriber. The subscriber profile information obtained from the HSS by the 'Cx-pull' during registration may contain complex logic and triggers causing session redirection. S-CSCF#2 sends the SIP INVITE request to the I-CSCF for the new destination (I-CSCF#F in the figure), who forwards it to S-CSCF#F, who forwards it to the new destination.

In cases when the destination subscriber is not currently registered in the IM CN subsystem, the I-CSCF may assign a temporary S-CSCF to perform the service control on behalf of the intended destination. This temporary S-CSCF takes the role of S-CSCF#2 in figure 10.4.2-1.

The service implemented by figure 10.4.2-1 is typically "Session Forward Unconditional", "Session Forward Variable" or "Selective Session Forwarding". S-CSCF#2 may also make use of knowledge of current sessions in progress at the UE, and implement "Session Forwarding Busy" in this way.

There are 9 distinct signalling flows for this session redirection, as follows:

- Single network operator performing origination, forwarding, and termination.
- One network operator performing origination and forwarding, separate network operator performing termination, with a THIG between to maintain configuration independence.
- One network operator performing origination and forwarding, separate network operator performing termination, without a THIG between.
- One network operator performing origination, second network operator performing forwarding and termination, with a THIG between to maintain configuration independence.
- One network operator performing origination, second network operator performing forwarding and termination, without a THIG between.
- One network operator performing origination, second network operator performing forwarding, and third network operator performing termination, without any THIGs between them.
- One network operator performing origination, second network operator performing forwarding, and third network operator performing termination, with a THIG between first two to maintain configuration independence
- One network operator performing origination, second network operator performing forwarding, and third network operator performing termination, with a THIG between second and third to maintain configuration independence.
- One network operator performing origination, second network operator performing forwarding, and third network operator performing termination, with a THIG between all three to maintain configuration independence.

Further, it is possible that a session will be redirected multiple times, so the above list generalizes to include multiple forwarding elements.

All of these Session-Redirection procedures can be combined with MO#1a, MO#1b, or MO#2 for session origination, and with MT#1a, MT#1b, or MT#2 for session termination.

Only the first case is shown here, with a single network operator performing origination, forwarding, and termination. The additional cases can be derived from the procedures shown here and in S-S#1a, and S-S#1b.

This case is shown in the signalling flow in figure 10.4.2-1.

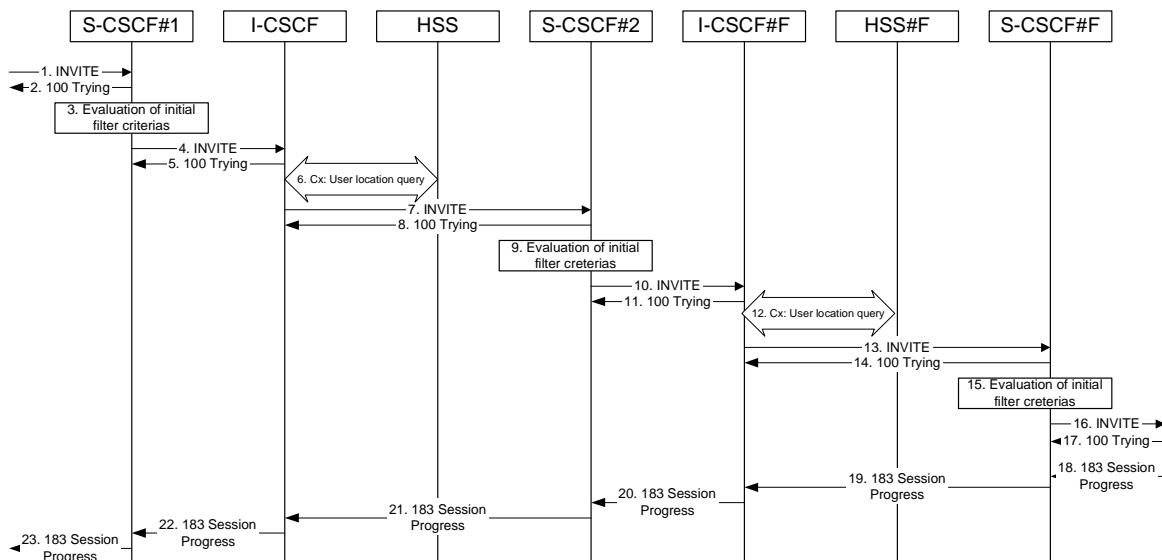


Figure 10.4.2-1: Session redirection initiated by S-CSCF to IM CN subsystem

The IM CN subsystem - Session Redirection Procedure is as follows:

1. INVITE (MO to S-CSCF) – see example in table 10.4.2-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 10.4.2-1: INVITE (MO to S-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Record-Route: <sip:pcscf1.home1.net;lr>
Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

2. 100 Trying (S-CSCF to MO) – see example in table 10.4.2-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 10.4.2-2: 100 Trying (S-CSCF to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criteria. For this example, assume no Application Server involvement.

4. INVITE (S-CSCF to I-CSCF) – see example in table 10.4.2-4

S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since it is a destination served by the same network operator, S-CSCF#1 forwards the INVITE request directly to I-CSCF in the same network.

Table 10.4.2-4: INVITE (S-CSCF to I-CSCF)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Request-URI: In the case where the Request-URI of the incoming INVITE request to S-CSCF contains a TEL-URL [5], it has to be translated to a globally routable SIP-URL before applying it as Request-URI of the outgoing INVITE request. For this address translation the S-CSCF uses the services of an ENUM-DNS protocol according to RFC 2916 [6], or any other suitable translation database. Database aspects of ENUM are outside the scope of this specification.

5. 100 Trying (I-CSCF to S-CSCF) – see example in table 10.4.2-5

I-CSCF responds to the INVITE request (4) by sending a 100 Trying provisional response to S-CSCF#1.

Table 10.4.2-5: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228 [11].

Table 7.3.2.1-6a provides the parameters in the SIP INVITE request (flow 4), which are sent to the HSS.

Table 7.3.2.1-6b provides the parameters sent from the HSS that need to be mapped to SIP INVITE (flow 7) and sent to S-CSCF.

7. INVITE (I-CSCF to S-CSCF) – see example in table 10.4.2-7

I-CSCF forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

Table 10.4.2-7: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Route: <sip:scscf2.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

NOTE 1: The I-CSCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

8. 100 Trying (S-CSCF to I-CSCF) – see example in table 10.4.2-8

S-CSCF#2 responds to the INVITE request (7) with a 100 Trying provisional response.

Table 10.4.2-8: 100 Trying (S-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

9. Evaluation of initial filter criterias

S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criterias. Based on some service-specific criterion, S-CSCF#2 decides to redirect this session attempt to a new IM CN subsystem destination, at the URL sip:user3_public1@home1.net.

10. INVITE (S-CSCF to I-CSCF) – see example in table 10.4.2-10

S-CSCF#2 performs an analysis of the destination address, and determines the new destination is served by the same network operator. S-CSCF#2 forwards the INVITE request directly to I-CSCF#3 (which may be different than I-CSCF#1 consulted earlier).

Table 10.4.2-10: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:user3_public1@home1.net;user=phone SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Record-Route: <sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

Request-URI: In the case where the Request-URI of the incoming INVITE request to S-CSCF contains a TEL-URL [5], it has to be translated to a globally routable SIP-URL before applying it as Request-URI of the outgoing INVITE request. For this address translation the S-CSCF uses the services of an ENUM-DNS protocol according to RFC 2916 [6], or any other suitable translation database. Database aspects of ENUM are outside the scope of this specification.

11. 100 Trying (I-CSCF to S-CSCF) – see example in table 10.4.2-11

I-CSCF responds to the INVITE request (10) by sending a 100 Trying provisional response to S-CSCF#1.

Table 10.4.2-11: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

12. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228 [11].

Table 7.3.2.1-6a provides the parameters in the SIP INVITE request (flow 10), which are sent to the HSS.

Table 7.3.2.1-6b provides the parameters sent from the HSS that need to be mapped to SIP INVITE (flow 13) and sent to S-CSCF.

13. INVITE (I-CSCF to S-CSCF) – see example in table 10.4.2-13

I-CSCF forwards the INVITE request to the S-CSCF (S-CSCF#3) that will handle the session termination.

15. Evaluation of initial filter criterias

S-CSCF#3 validates the service profile of this subscriber and evaluates the initial filter criterias.

16. INVITE (S-CSCF to MT) – see example in table 10.4.2-16

S-CSCF#3 forwards the INVITE request, as determined by the termination procedure. S-CSCF#3 remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE.

Table 10.4.2-16: INVITE (S-CSCF to MT)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf3.home1.net;branch=z9hG4bKyiiir82.4, SIP/2.0/UDP
    icscf3_s.home1.net;branch=z9hG4bK87rr82.1, SIP/2.0/UDP
    scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 64
Record-Route: <sip:scscf3.home1.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Route: <sip:pcscf3.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
P-Called-Party-ID: <sip:user3_public1@home1.net>
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

17. 100 Trying (MT to S-CSCF) – see example in table 10.4.2-17

S-CSCF#2 receives a 100 Trying provisional response to the INVITE request, as specified by the termination procedures.

Table 10.4.2-17: 100 Trying (MT to S-S#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf3.home1.net;branch=z9hG4bKyiiir82.4, SIP/2.0/UDP
    icscff.home1.net;branch=z9hG4bK87rr82.1, SIP/2.0/UDP
    scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

18. 183 Session Progress (MT to S-CSCF) – see example in table 10.4.2-18

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response, as per the termination procedure.

Table 10.4.2-18: 183 Session Progress (MT to S-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf3.home1.net;branch=z9hG4bKyiiir82.4, SIP/2.0/UDP
    icscf3_s.home1.net;branch=z9hG4bK87rr82.1, SIP/2.0/UDP
    scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Record-Route: <sip:pcscf3.home1.net;lr>, <sip:scscf3.home1.net;lr>,
    <sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Smith" <tel:+1-212-555-3333>
Privacy: none
P-Charging-Vector:
From:
To: <tel:+1-212-555-2222>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```


P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

19. 183 Session Progress (S-CSCF to I-CSCF) – see example in table 10.4.2-19

S-CSCF#2 forwards the 183 Session Progress provisional response to I-CSCF.

Table 10.4.2-19: 183 Session Progress (S-CSCF to I-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf3_s.home1.net;branch=z9hG4bK87rr82.1, SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKKnashds7
Record-Route:
P-Asserted-Identity: "John Smith" <tel:+1-212-555-3333>
Privacy: none
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Supported:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

20. 183 Session Progress (I-CSCF to S-CSCF) – see example in table 10.4.2-20

I-CSCF forwards the 183 Session Progress provisional response to S-CSCF#1.

Table 10.4.2-20: 183 Session Progress (I-CSCF to S-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Supported:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

21. 183 Session Progress (S-CSCF to I-CSCF) – see example in table 10.4.2-21

S-CSCF#2 forwards the 183 Session Progress provisional response to I-CSCF.

Table 10.4.2-21: 183 Session Progress (S-CSCF to I-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Supported:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

22. 183 Session Progress (I-CSCF to S-CSCF) – see example in table 10.4.2-22

I-CSCF forwards the 183 Session Progress provisional response to S-CSCF#1.

Table 10.4.2-22: 183 Session Progress (I-CSCF to S-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Supported:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

23. 183 Session Progress (S-CSCF to MO) – see example in table 10.4.2-23

S-CSCF#1 forwards the 183 Session Progress to the originator, as per the originating procedure.

Table 10.4.2-23: 183 Session Progress (S-CSCF to MO)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscfl.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Supported:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

PROPOSED CHANGE

10.4.3 Session redirection initiated by S-CSCF to CS-domain (S-S#2, MT#2 assumed)

The S-CSCF in the scenario above may determine that the session is to be redirected to a CS-domain endpoint, or to the PSTN. It recognizes this situation by the redirected URL being a tel: URL.

For the simplest configuration (Mobile located in home service area (MO#2), initiating a session to a destination served by same network operator(S-S#2)), the handling of redirection to a tel: URL is shown in figure 10.4.3-1. Other cases, which include roaming, PSTN origination, destinations served by other network operators, and THIGs, are handled in a similar manner.

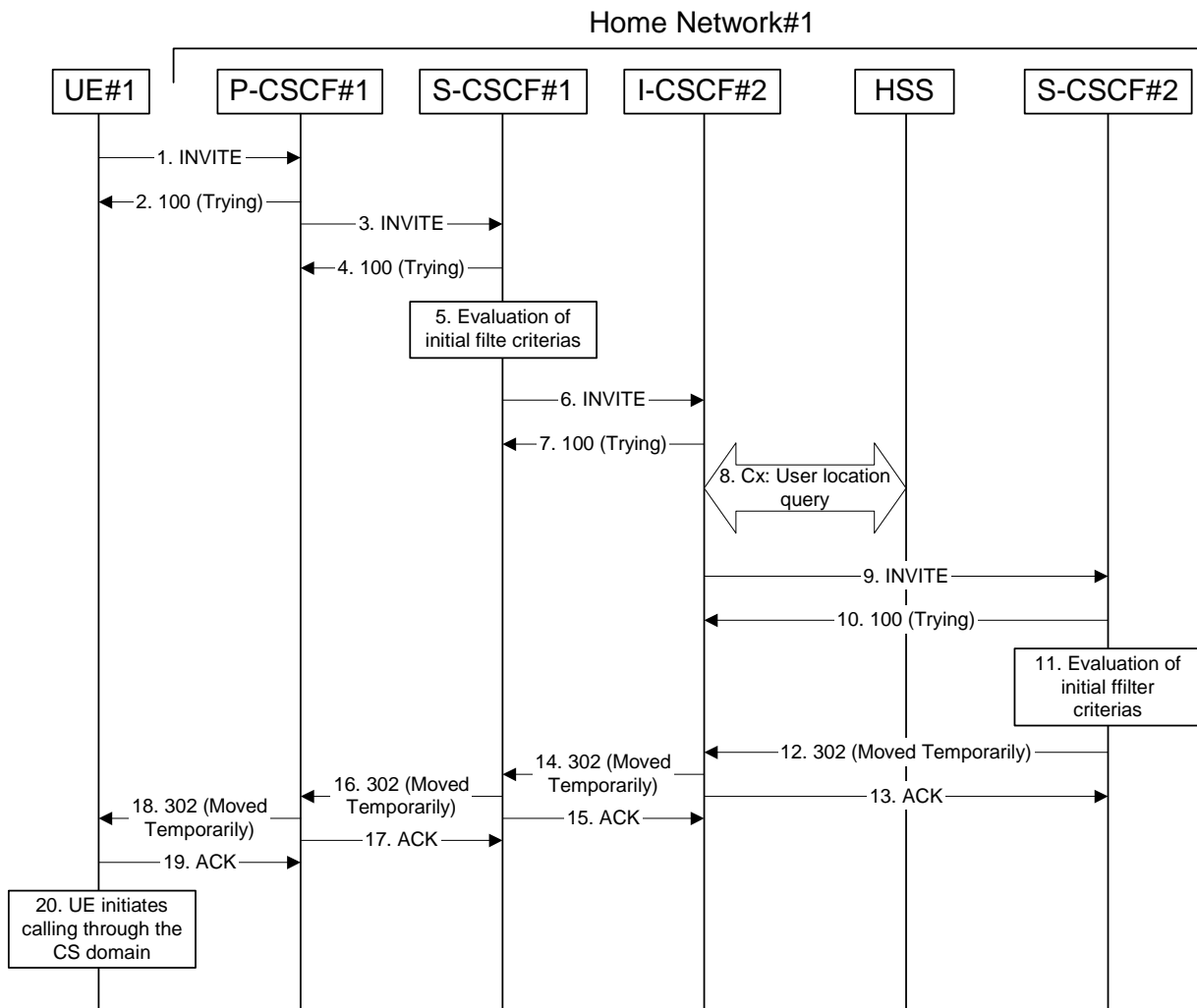


Figure 10.4.3-1: Session redirection initiated by S-CSCF to CS-Domain

Step-by-step processing is as follows:

1. INVITE (UE to P-CSCF) – see example in table 10.4.3-1

UE sends the INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism.

Table 10.4.3-1: INVITE (UE to P-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
    port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtmap:96 telephone-event
a=maxptime:20

```

Request-URI: Contains the keyed number from the user.

Via: Contains the IP address or FQDN of the originating UE.

P-Preferred-Identity: the user provides a hint about the identity to be used for this session.

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

From:/To:/Call-ID: Follow the recommendations of RFC 3323 [13], even though anonymity is not being requested for this session.

Cseq: is a random starting number.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

Contact: is a SIP URI that contains the IP address or FQDN of the originating UE.

2. 100 Trying (P-CSCF to UE) – see example in table 10.4.3-2

P-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 10.4.3-2: 100 Trying (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. INVITE (P-CSCF to S-CSCF) – see example in table 10.4.3-3

The P-CSCF adds itself to the Record-Route header and Via header.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

The INVITE request is forwarded to the S-CSCF.

Table 10.4.3-3: INVITE (P-CSCF to S-CSCF)

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Record-Route: <sip:pcscf1.home1.net;lr>
Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Require: precondition
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Access-Network-Info: this header contains information from the UE.

4. 100 Trying (S-CSCF to P-CSCF) – see example in table 10.4.3-4

S-CSCF responds to the INVITE request (3) with a 100 Trying provisional response.

Table 10.4.3-4: 100 Trying (S-CSCF to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

5. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber and evaluates the initial filter criterias.

6. INVITE (S-CSCF to I-CSCF) – see example in table 10.4.3-6

S-CSCF forwards the INVITE request, as specified by the S-CSCF to S-CSCF procedures.

Table 10.4.3-6: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>;
Privacy: none
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Request-URI: In the case where the Request-URI of the incoming INVITE request to S-CSCF contains a TEL-URL [5], it has to be translated to a globally routable SIP-URL before applying it as Request-URI of the outgoing INVITE request. For this address translation the S-CSCF uses the services of an ENUM-DNS protocol according to RFC 2916 [6], or any other suitable translation database. Database aspects of ENUM are outside the scope of this specification.

7. 100 Trying (I-CSCF to S-CSCF) – see example in table 10.4.3-7

S-CSCF receives a 100 Trying provisional response, as specified by the S-CSCF to S-CSCF procedures.

Table 10.4.3-7: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

8. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228 [11].

Table 7.3.2.1-6a provides the parameters in the SIP INVITE request (flow 6), which are sent to the HSS.

Table 7.3.2.1-6b provides the parameters sent from the HSS that need to be mapped to SIP INVITE (flow 9) and sent to S-CSCF.

9. INVITE (I-CSCF to S-CSCF) – see example in table 10.4.3-9

I-CSCF forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

Table 10.4.3-9: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Route: <sip:scscf2.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

NOTE: The I-CSCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

Remainder of subclause not shown

PROPOSED CHANGE

10.4.4 Session redirection initiated by S-CSCF to general endpoint (S-S#2, MT#2 assumed)

The S-CSCF in the scenario above may determine that the session is to be redirected to an endpoint outside the IMS and outside the CS-domain. Examples of these destinations include web pages, email addresses, etc. It recognizes this situation by the redirected URL being other than a sip: or tel: URL.

For the simplest configuration (Mobile located in home service area (MO#2), initiating a session to a destination served by same network operator(S-S#2)), the handling of redirection to a general URL is shown in figure 10.4.4-1. Other cases, which include roaming, PSTN origination, destinations served by other network operators, and THIGs, are handled in a similar manner.

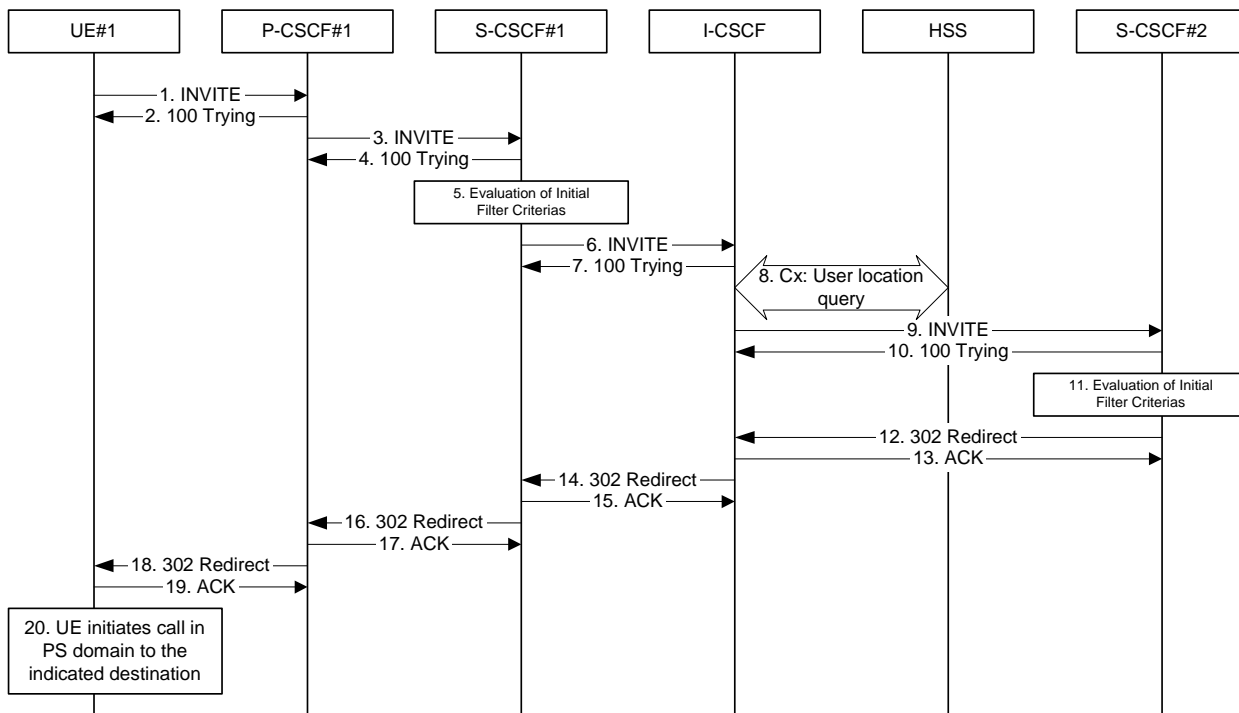


Figure 10.4.4-1: Session redirection initiated by S-CSCF to general endpoint

Step-by-step processing is as follows:

1. INVITE (UE to P-CSCF) – see example in table 10.4.4-1

UE sends the INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism.

Table 10.4.4-1: INVITE (UE to P-CSCF)

```

INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
    port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
a=rtptime:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

Request-URI: Contains the keyed number from the user.

Via: Contains the IP address or FQDN of the originating UE.

P-Preferred-Identity: the user provides a hint about the identity to be used for this session.

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

Route: contains the P-CSCF address learnt during P-CSCF discovery, plus the elements from the Service-Route header from registration. The P-CSCF URI contains the port number learnt during the security agreement negotiation

From:/To:/Call-ID: Follow the recommendations of RFC 3323 [13], even though anonymity is not being requested for this session.

Cseq: is a random starting number.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

Contact: is a SIP URI that contains the IP address or FQDN of the originating UE.

2. 100 Trying (P-CSCF to UE) – see example in table 10.4.4-2

P-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 10.4.4-2: 100 Trying (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. INVITE (P-CSCF to S-CSCF) – see example in table 10.4.4-3

The P-CSCF adds itself to the Record-Route header and Via header. As the request is forwarded to an interface that is not compressed, the own P-CSCF SIP URI does not contain the "comp=sigcomp" parameter.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

The INVITE request is forwarded to the S-CSCF.

Table 10.4.4-3: INVITE (P-CSCF to S-CSCF)

```
INVITE tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Record-Route: <sip:pcscf1.home1.net;lr>
Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Require: preconditions
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Access-Network-Info: this header contains information from the UE.

4. **100 Trying (S-CSCF to P-CSCF) – see example in table 10.4.4-4**

S-CSCF responds to the INVITE request (3) with a 100 Trying provisional response.

Table 10.4.4-4: 100 Trying (S-CSCF to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

5. **Evaluation of initial filter criterias**

S-CSCF validates the service profile of this subscriber and evaluates the initial filter criterias.

6. **INVITE (S-CSCF to I-CSCF) – see example in table 10.4.4-6**

S-CSCF forwards the INVITE request, as specified by the S-CSCF to S-CSCF procedures.

Table 10.4.4-6: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>;
Privacy: none
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Request-URI: In the case where the Request-URI of the incoming INVITE request to S-CSCF contains a TEL-URL [5], it has to be translated to a globally routable SIP-URL before applying it as Request-URI of the outgoing INVITE request. For this address translation the S-CSCF uses

the services of an ENUM-DNS protocol according to RFC 2916 [6], or any other suitable translation database. Database aspects of ENUM are outside the scope of this specification.

7. 100 Trying (I-CSCF to S-CSCF) – see example in table 10.4.4-7

S-CSCF receives a 100 Trying provisional response, as specified by the S-CSCF to S-CSCF procedures.

Table 10.4.4-7: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

8. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228 [11].

Table 7.3.2.1-6a provides the parameters in the SIP INVITE request (flow 6), which are sent to the HSS.

Table 7.3.2.1-6b provides the parameters sent from the HSS that need to be mapped to SIP INVITE (flow 9) and sent to S-CSCF.

9. INVITE (I-CSCF to S-CSCF) – see example in table 10.4.4-9

I-CSCF forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

Table 10.4.4-9: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Route: <sip:scscf2.home1.net;lr>
Supported:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

NOTE: The I-CSCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

Remainder of subclause not shown

PROPOSED CHANGE

10.4.7 Session redirection initiated after bearer establishment

The UE of the destination subscriber may request the session be redirected after a customer-specified ringing interval. The UE may also implement customer-specific feature processing, and base its decision to redirect this session on such things as the identity of caller, current sessions in progress, other applications currently being accessed, etc. The UE sends the SIP Redirect response to its P-CSCF, who forwards back along the signalling path to the originating endpoint, who initiates a session to the new destination.

The service implemented by this signalling flow is typically "Session Forward No Answer".

Redirection to another CN subsystem endpoint (e.g. a sip: URL) is shown in figure 10.4.7-1. The figure starts at the point in the session establishment when the destination is known, resources have been reserved, and the destination subscriber is being alerted. If the desire for redirection was known earlier than this point, the procedures of Subclause 10.4.6 would be followed instead.

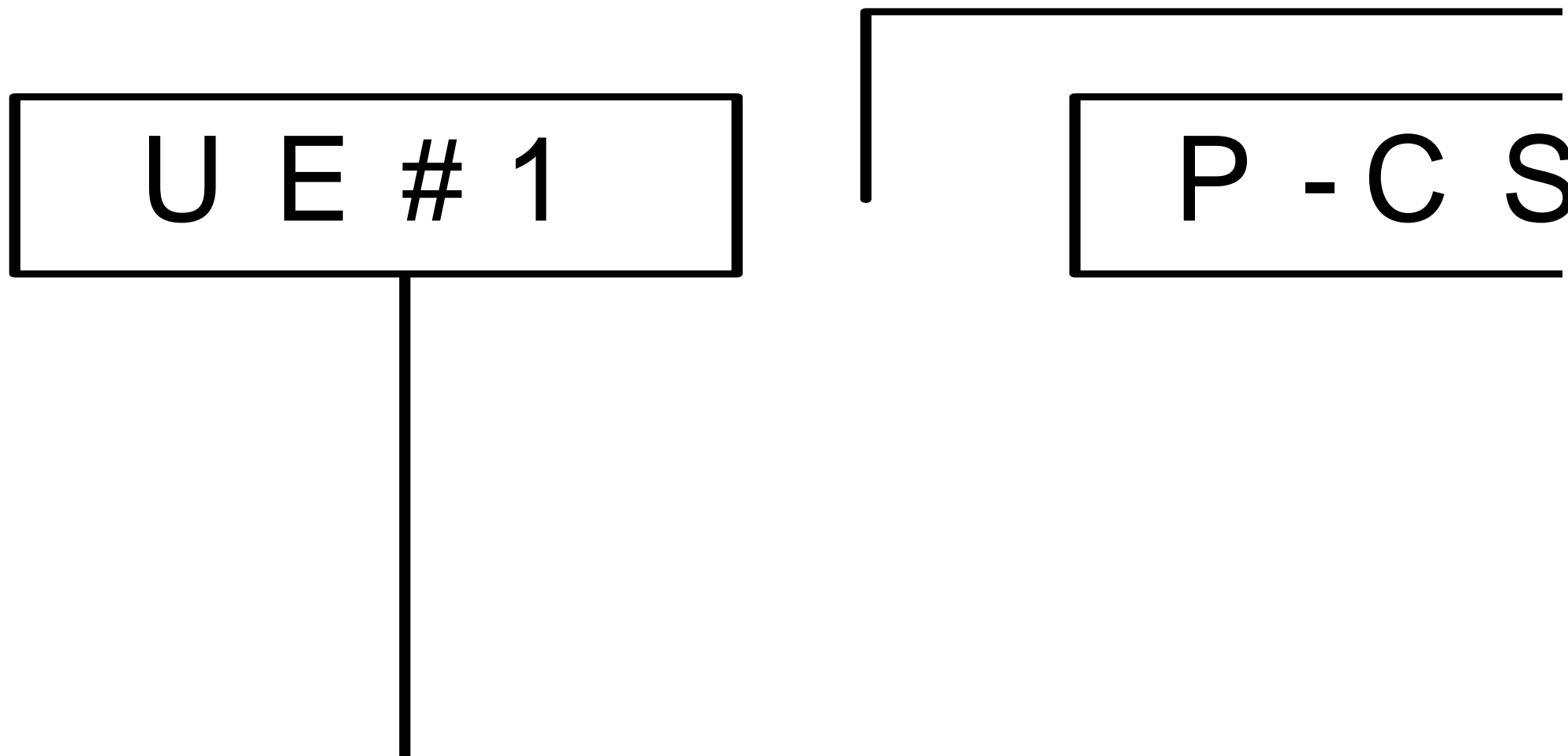


Figure 10.4.7-1: Session redirection after bearer establishment

Step-by-step processing is as follows:

1. **180 Ringing (UE to P-CSCF) – see example in table 10.4.7-1**

Depending on the type of codec change being performed, alerting may be required at the destination UE. If so, UE#2 sends a 180 Ringing provisional response to the originator, through P-CSCF#2.

Table 10.4.7-1: 180 Ringing (UE to P-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP pcscf2.home1.net:5088;comp=sigcomp;branch=z9hG4bK556g98.5, SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.home1.net:5088;lr;comp=sigcomp>, <sip:scscf2.home1.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222;tag=314159>
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 131 INVITE
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 19
Content-Length: 0
```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

2. **180 Ringing (P-CSCF to S-CSCF) – see example in table 10.4.7-2**

P-CSCF#2 sends the 180 Ringing response to S-CSCF#2.

Table 10.4.7-2: 180 Ringing (P-CSCF to S-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
Record-Route: <sip:pcscf2.home1.net;lr>, <sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.home1.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrBHLso=023551024";
ggsn=[5555::d6d:c7c:b8b:a9a]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-sig=no;
gcid=A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no; gcid=F312D5E3BC; flow-
id=({2,1},{2,2})"
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Length:
```

P-Access-Network-Info: This header contains information from the UE.

3. **180 Ringing (S-CSCF to I-CSCF) – see example in table 10.4.7-3**

S-CSCF#2 sends the 180 Ringing response to I-CSCF#2.

Table 10.4.7-3: 180 Ringing (S-CSCF to I-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Length:
```

4. 180 Ringing (I-CSCF to S-CSCF) – see example in table 10.4.7-4

I-CSCF#2 sends the 180 Ringing response to S-CSCF#1.

Table 10.4.7-4: 180 Ringing (I-CSCF to S-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Length:
```

5. 180 Ringing (S-CSCF to P-CSCF) – see example in table 10.4.7-5

S-CSCF#1 sends the 180 Ringing response to P-CSCF#1.

Table 10.4.7-5: 180 Ringing (S-CSCF to P-CSCF)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Length:
```

6. 180 Ringing (P-CSCF to UE) – see example in table 10.4.7-6

P-CSCF#1 sends the 180 Ringing response to UE#1.

Table 10.4.7-6: 180 Ringing (P-CSCF to UE)

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Length:
```

7. PRACK (UE to P-CSCF) – see example in table 10.4.7-7

UE#1 sends the PRACK request to UE#2, along the signalling path established by the INVITE request.

Table 10.4.7-7: PRACK (UE to P-CSCF)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
<sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 130 PRACK
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
RAck: 19 131 INVITE
Content-Length: 0
```

Request-URI: Takes the value of the Contact header of the 180 Ringing response.

P-Access-Network-Info: The UE provides the access-type and access-info, related to the serving access network.

Via: Take the value of either the IP address or FQDN of the UE.

From:/To:/Call-ID: Copied from the 180 Ringing response so that they include any revised tag parameters.

Cseq: Takes a higher value than in the previous request.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

8. PRACK (P-CSCF to S-CSCF) – see example in table 10.4.7-8

P-CSCF#1 sends the PRACK request to S-CSCF#1, along the signalling path established by the INVITE request.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

Table 10.4.7-8: PRACK (P-CSCF to S-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pscsf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
P-Access-Network-Info:
From:
To:
Call-ID:
Cseq:
Contact:
RAck:
Content-Length:

```

P-Access-Network-Info: This header contains information from the UE.

9. PRACK (S-CSCF to S-CSCF) – see example in table 10.4.7-9

S-CSCF#1 sends the PRACK request to S-CSCF#2, along the signalling path established by the INVITE request.

Table 10.4.7-9: PRACK (S-CSCF to S-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Contact:
RAck:
Content-Length:

```

10. PRACK (S-CSCF to P-CSCF) – see example in table 10.4.7-10

S-CSCF#2 sends the PRACK request to P-CSCF#2, along the signalling path established by the INVITE request.

Table 10.4.7-10: PRACK (S-CSCF to P-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Contact:
RAck:
Content-Length:

```

11. PRACK (P-CSCF to UE) – see example in table 10.4.7-11

P-CSCF#2 sends the PRACK request to UE#2, along the signalling path established by the INVITE request.

Table 10.4.7-11: PRACK (P-CSCF to UE)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home1.net:5088;comp=sigcomp;branch=z9hG4bK526mj01.5, SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
Cseq:
Contact:
RAck:
Content-Length:

```

12. 200 OK (UE to P-CSCF) – see example in table 10.4.7-12

UE#2 responds to the PRACK request (11) with a 200 OK response to P-CSCF#2.

Table 10.4.7-12: 200 OK (UE to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home1.net:5088;comp=sigcomp;branch=z9hG4bK526mj01.5, SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

13. 200 OK (P-CSCF to S-CSCF) – see example in table 10.4.7-13

P-CSCF#2 sends the 200 OK response to S-CSCF#2.

Table 10.4.7-13: 200 OK (P-CSCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Length:

```

14. 200 OK (S-CSCF to S-CSCF) – see example in table 10.4.7-14

S-CSCF#2 sends the 200 OK response to S-CSCF#1.

Table 10.4.7-14: 200 OK (S-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

15. 200 OK (S-CSCF to P-CSCF) – see example in table 10.4.7-15

S-CSCF#1 sends the 200 OK response to P-CSCF#1.

Table 10.4.7-15: 200 OK (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

16. 200 OK (P-CSCF to UE) – see example in table 10.4.7-16

P-CSCF#1 sends the 200 OK response to UE#1.

Table 10.4.7-16: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

17. 302 Moved Temporarily (UE to P-CSCF) – see example in table 10.4.7-17

Based on some service criterion, such as a timeout value, UE#2 decides to redirect this session request to another destination. UE#2 sends a 302 Moved Temporarily response to P-CSCF, containing the new destination. For this example, consider the new destination to be <tel:+1-212-555-3333>.

Table 10.4.7-17: 302 Moved Temporarily (UE to P-CSCF)

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP pcscf2.home1.net:5088;comp=sigcomp;branch=z9hG4bK523r01.2, SIP/2.0/UDP
    scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Contact: <tel:+1-212-555-3333>
Content-Length: 0
```

18. ACK (P-CSCF to UE) – see example in table 10.4.7-18

P-CSCF acknowledges receipt of the 302 Moved Temporarily response (17) by sending an ACK request to UE#2.

Table 10.4.7-18: ACK (P-CSCF to UE)

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home1.net:5088;comp=sigcomp;branch=z9hG4bK523r01.2
Max-Forwards: 70
From:
To:
Call-ID:
Cseq:
Content-Length:
```

19. Revoke QoS

P-CSCF revokes any authorization is had made for Quality of Service for this session.

20. 302 Moved Temporarily (P-CSCF to S-CSCF) – see example in table 10.4.7-20

P-CSCF#2 sends a 302 (Moved Temporarily) response to S-CSCF#2, containing the new destination.

Table 10.4.7-20: 302 Moved Temporarily (P-CSCF to S-CSCF)

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:5088;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

21. ACK (S-CSCF to P-CSCF) – see example in table 10.4.7-21

S-CSCF acknowledges receipt of the 302 (Moved Temporarily) response (20) by sending an ACK request to P-CSCF#2.

Table 10.4.7-21: ACK (S-CSCF to P-CSCF)

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1
Max-Forwards:70
Route: <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

22. 302 Moved Temporarily (S-CSCF to I-CSCF) – see example in table 10.4.7-22

S-CSCF#2 sends a 302 (Moved Temporarily) response to I-CSCF, containing the updated destination.

Table 10.4.7-22: 302 Moved Temporarily (S-CSCF to I-CSCF)

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact: <sip:Token(tel:+1-212-555-3333)@scscf3.home1.net;lr;tokenized-by=scscf2.home1.net>
Content-Length:
```

23. ACK (I-CSCF to S-CSCF) – see example in table 10.4.7-23

I-CSCF acknowledges receipt of the 302 (Moved Temporarily) response (22) by sending an ACK request to S-CSCF#2.

Table 10.4.7-23: ACK (I-CSCF to S-CSCF)

```
ACK tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK09a238.1
Route: <sip:scscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

24. 302 Moved Temporarily (I-CSCF to S-CSCF) – see example in table 10.4.7-24

I-CSCF may (based on operator preferences) update the new destination address, in order to hide the S-CSCF address and maintain configuration independence. If so, it generates a new private URL with its own hostname. I-CSCF sends a 302 (Moved Temporarily) response to S-CSCF#1, containing the new destination.

Table 10.4.7-24: 302 Moved Temporarily (I-CSCF to S-CSCF)

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact: <sip:Token(token(tel:+1-212-555-3333)@scscf3.home1.net;lr;tokenized-
    by=scscf2.home1.net)@icscf3_s.home1.net;lr;tokenized-by=icscf2_s.home1.net>
Content-Length: 0
```

25. ACK (S-CSCF to I-CSCF) – see example in table 10.4.7-25

S-CSCF#1 acknowledges receipt of the 302 (Moved Temporarily) response (24) by sending an ACK request to I-CSCF.

Table 10.4.7-25: ACK (S-CSCF to I-CSCF)

```
ACK tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1
Mas-Forwards: 70
Route: <sip:icscf2_s.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

26. 302 Moved Temporarily (S-CSCF to P-CSCF) – see example in table 10.4.7-26

S-CSCF#1 sends a 302 (Moved Temporarily) response to P-CSCF, containing the new destination.

Table 10.4.7-26 302 Moved Temporarily (S-CSCF to P-CSCF)

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length: 0
```

27. ACK (P-CSCF to S-CSCF) – see example in table 10.4.7-27

P-CSCF acknowledges receipt of the 302 (Moved Temporarily) response (26) by sending an ACK request to S-CSCF#1.

Table 10.4.7-27: ACK (P-CSCF to S-CSCF)

```
ACK tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1
Max-Forwards: 70
Route: <sip:scscf1.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

28. 302 Moved Temporarily (P-CSCF to UE) – see example in table 10.4.7-28

P-CSCF sends a 302 (Moved Temporarily) response to UE, containing the new destination.

Table 10.4.7-28: 302 Moved Temporarily (P-CSCF to UE)

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length: 0
```

29. ACK (UE to P-CSCF) – see example in table 10.4.7-29

UE acknowledges receipt of the 302 (Moved Temporarily) response (28) by sending an ACK request to P-CSCF.

Table 10.4.7-29: ACK (UE to P-CSCF)

```
ACK tel:+1-212-555-2222 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

30. INVITE (UE to P-CSCF) – see example in table 10.4.7-30

UE sends the INVITE request, containing an initial SDP and the new destination, to the P-CSCF determined via the CSCF discovery mechanism.

Table 10.4.7-30: INVITE (UE to P-CSCF)

```

INVITE sip:Token(token(tel:+1-212-555-3333)@scscf2.home1.net;lr;tokenized-
  by=scscf2.home1.net)@icscf2_s.home1.net;lr;tokenized-by=icscf2_s.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
  c=8642; port-s=7531
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0_0
m=audio 3456 RTP/AVP 97 3 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 G726-32/8000
a=rtpmap:96 telephone-event
a=maxptime:20

```

Request-URI: Contains the SIP URI from the Contact header in the received 302 (Moved Temporarily) response.

Via: Contains the IP address or FQDN of the originating UE.

P-Preferred-Identity: the user provides a hint about the identity to be used for this session.

P-Access-Network-Info: The UE provides the access-type and access-info, related to the serving access network.

From:/To:/Call-ID: Follow the recommendations of RFC 3323 [13], even though privacy is not being requested for this session.

Cseq: is a random starting number.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

Contact: is a SIP URI that contains the IP address or FQDN of the originating UE.

31. 100 Trying (P-CSCF to UE) – see example in table 10.4.7-31

P-CSCF responds to the INVITE request (30) with a 100 (Trying) provisional response.

Table 10.4.7-31: 100 Trying (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

32. INVITE (P-CSCF to S-CSCF) – see example in table 10.4.7-32

The P-CSCF adds itself to the Record-Route header, and adds a Via header.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

The INVITE request is forwarded to the S-CSCF.

Table 10.4.7-32: INVITE (P-CSCF to S-CSCF)

```
INVITE sip:Token(token(tel:+1-212-555-3333)@scscf2.home1.net;lr;tokenized-
by=scscf2.home1.net)@icscf2_s.home1.net;lr;tokenized-by=icscf2_s.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Record-Route: <sip:pcscf1.home1.net;lr>
Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Require: precondition
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Access-Network-Info: this header contains information from the UE.

33. 100 Trying (S-CSCF to P-CSCF) – see example in table 10.4.7-33

S-CSCF responds to the INVITE request (32) with a 100 (Trying) provisional response.

Table 10.4.7-33: 100 Trying (S-CSCF to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

34. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias. In this example it is assume that no application server is involved.

35. INVITE (S-CSCF to I-CSCF) – see example in table 10.4.7-35

S-CSCF forwards the INVITE request to the I-CSCF specified in the destination URL.

Table 10.4.7-35: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:Token(token(tel:+1-212-555-3333)@scscf2.home1.net;lr;tokenized-
    by=scscf2.home1.net)@icscf2_s.home1.net;lr;tokenized-by=icscf2_s.home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Request-URI: This is the private URL obtained from the previous 302 (Moved Temporarily) response, which identifies the I-CSCF that must first translate the destination (then the S-CSCF that must further translate the destination).

36. 100 Trying (I-CSCF to S-CSCF) – see example in table 10.4.7-36

I-CSCF responds to the INVITE request (35) with a 100 (Trying) provisional response.

Table 10.4.7-36: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

37. INVITE (I-CSCF to S-CSCF) – see example in table 10.4.7-37

I-CSCF translates the private portion of the URL, and determines the destination is S-CSCF#2. I-CSCF forwards the INVITE request to the S-CSCF#2 that will further translate the destination.

Table 10.4.7-37: INVITE (I-CSCF to S-CSCF)

```
INVITE sip:Token(tel:+1-212-555-3333)@scscf2.home1.net;lr;tokenized-by=scscf2.home1.net
SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

38. 100 Trying (S-CSCF to I-CSCF) – see example in table 10.4.7-38

S-CSCF#2 responds to the INVITE request (37) with a 100 (Trying) provisional response.

Table 10.4.7-38: 100 Trying (S-CSCF to I-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

39. INVITE (S-CSCF to I-CSCF) – see example in table 10.4.7-39

S-CSCF#2 translates the private portion of the URL, and determines the destination address. S-CSCF#2 forwards the INVITE request to the I-CSCF#3, the entry point to the destination operator's network.

Table 10.4.7-39: INVITE (S-CSCF to I-CSCF)

```
INVITE tel:+1-212-555-3333 SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK09a238.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Record-Route: <sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Route: <sip:icscf3_s.home3.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Remainder of subclause not shown

PROPOSED CHANGE

10.5.2 Session Transfer initiating a new session

An IM session already exists between UE#1 and UE#2. UE#2 desires UE#1 to initiate a new session to a new destination, UE#3, and terminate the existing session. The procedures for this transfer are shown in figure 10.5.2-1.

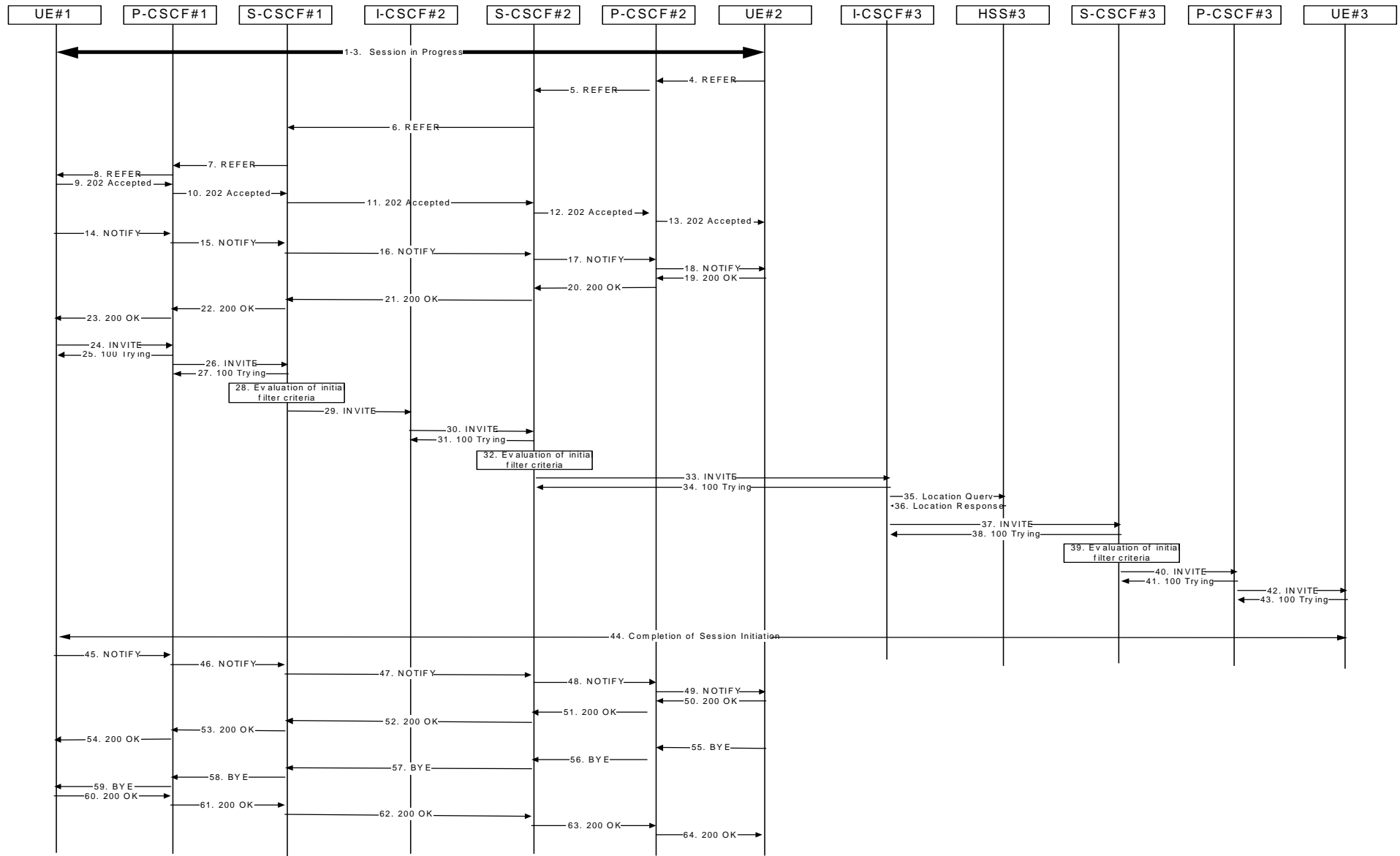


Figure 10.5.2-1: Session Transfer initiating a new session

1-3. Session in Progress

UE#1 initiates a multimedia session with UE#2. As a result, the state information stored at P-CSCF#2 is shown in table 10.5.2-1.

Table 10.5.2-1: State Information

```
Request-URI: sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+602IrT5tAFrbHLso=023551024"
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

4. REFER (UE to P-CSCF) – see example in table 10.5.2-4

UE#2 sends a REFER request to its proxy, P-CSCF#2.

Table 10.5.2-4: REFER (UE to P-CSCF)

```
REFER sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::eee:fff:aaa:bbb]:8805;comp=sigcomp;branch=z9hG4bK834y72.2
Max-Forwards: 70
Route: <sip:pcscf2.home2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
      <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Preferred-Identity: "John Smith" <tel:+1-212-555-2222>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <tel:+1-212-555-2222>;tag=314159
To: <sip:user1_public1@home1.net>;tag=171828
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 130 REFER
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c= 22334455; spi-s=11223344; port-
c=6199; port-s=5088
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Refer-To: <tel:+1-212-555-3333>
Content-Length: 0
```

Request-URI: Contains the value of the Contact header from the initial INVITE.

Via: Contains the IP address or FQDN of the originating UE.

Privacy: the user does not require privacy, therefore the Privacy header is set to the value "none" as specified in RFC 3325 [17] and RFC 3323 [13].

P-Preferred-Identity: the user provides a hint about the identity to be used for this session.

P-Access-Network-Info: The UE provides the access-type and access-info, related to the serving access network.

From:/To:/Call-ID: Contain the values previously used to establish the session, including the tag value from the response.

Cseq: Next higher sequential value.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

Contact: is a SIP URI that contains the IP address or FQDN of the originating UE.

5. REFER (P-CSCF to S-CSCF) – see example in table 10.5.2-5

P-CSCF#2 forwards the Refer request to S-CSCF#2.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

Table 10.5.2-5: REFER (P-CSCF to S-CSCF)

```
REFER sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    [5555::eee:fff:aaa:bbb]:8805;comp=sigcomp;branch=z9hG4bK834y72.2
Max-Forwards: 69
Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Smith" <tel:+1-212-555-2222>
P-Access-Network-Info:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Contact:
Refer-To:
Content-Length:
```

P-Access-Network-Info: this header contains information from the UE.

Contact: Contains a SIP URI with the IP address or FQDN of the UE.

6. REFER (S-CSCF to S-CSCF) – see example in table 10.5.2-6

In order to maintain the expectation of privacy of the identity of the new destination, S-CSCF#2 converts the "Refer-To" header into a private URL. S-CSCF#2 forwards the Refer request to S-CSCF#1.

Table 10.5.2-6: REFER (S-CSCF to S-CSCF)

```
REFER sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    [5555::eee:fff:aaa:bbb]:8805;comp=sigcomp;branch=z9hG4bK834y72.2
Max-Forwards: 68
Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Contact:
Refer-To: <sip:token(tel:+1-212-555-3333)@scscf2.home2.net;lr;tokenized-by=scscf2.home2.net>
Content-Length:
```

7. REFER (S-CSCF to P-CSCF) – see example in table 10.5.2-7

S-CSCF#1 forwards the Refer request to P-CSCF#1.

Table 10.5.2-7: REFER (S-CSCF to P-CSCF)

```

REFER sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    [5555::eee:fff:aaa:bbb]:8805;comp=sigcomp;branch=z9hG4bK834y72.2
Max-Forwards: 67
Route: <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Contact:
Refer-To:
Content-Length:

```

8. REFER (P-CSCF to UE) – see example in table 10.5.2-8

P-CSCF#1 forwards the Refer request to UE#1.

Table 10.5.2-8: REFER (P-CSCF to UE)

```

REFER sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net:7531;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    [5555::eee:fff:aaa:bbb]:8805;comp=sigcomp;branch=z9hG4bK834y72.2
Max-Forwards: 66
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Refer-To:
Content-Length:

```

9. 202-Accepted (UE to P-CSCF) – see example in table 10.5.2-9

UE#2 acknowledges receipt of the REFER request (8) with a 202 (Accepted) final response, sent to P-CSCF#1.

Table 10.5.2-9: 202 (Accepted) (UE to P-CSCF)

```

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP pcscf1.home1.net:7531;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    [5555::eee:fff:aaa:bbb]:8805;comp=sigcomp;branch=z9hG4bK834y72.2
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Length: 0

```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

10. 202-Accepted (P-CSCF to S-CSCF) – see example in table 10.5.2-10

P-CSCF#1 forwards the 202 (Accepted) final response to S-CSCF#1.

Table 10.5.2-10: 202 (Accepted) (P-CSCF to S-CSCF)

```
SIP/2.0 202 Accepted
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    [5555::eee:fff:aaa:bbb]:1357;comp=sigcomp;branch=z9hG4bK834y72.2
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

P-Access-Network-Info: This header contains information from the UE.

11. 202-Accepted (S-CSCF to S-CSCF) – see example in table 10.5.2-11

S-CSCF#1 forwards the 202 (Accepted) final response to S-CSCF#2.

Table 10.5.2-11: 202 (Accepted) (S-CSCF to S-CSCF)

```
SIP/2.0 202 Accepted
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    [5555::eee:fff:aaa:bbb]:1357;comp=sigcomp;branch=z9hG4bK834y72.2
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

12. 202-Accepted (S-CSCF to P-CSCF) – see example in table 10.5.2-12

S-CSCF#2 forwards the 202 (Accepted) final response to P-CSCF#2.

Table 10.5.2-12: 202 (Accepted) (S-CSCF to P-CSCF)

```
SIP/2.0 202 Accepted
Via: SIP/2.0/UDP pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    [5555::eee:fff:aaa:bbb]:1357;comp=sigcomp;branch=z9hG4bK834y72.2
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

13. 202-Accepted (P-CSCF to UE) – see example in table 10.5.2-13

P-CSCF#2 forwards the 202 (Accepted) final response to UE#2.

Table 10.5.2-13: 202 (Accepted) (P-CSCF to UE)

```
SIP/2.0 202 Accepted
Via: SIP/2.0/UDP [5555::eee:fff:aaa:bbb]:1357;comp=sigcomp;branch=z9hG4bK834y72.2
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

14. NOTIFY (UE to P-CSCF) – see example in table 10.5.2-14

UE#1 sends an immediate NOTIFY request to its proxy, P-CSCF#1.

Table 10.5.2-14: NOTIFY (UE to P-CSCF)

```
NOTIFY sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
<sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
Cseq: 130 NOTIFY
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:8805;comp=sigcomp>
Subscription-State: active;expires=240
Event: refer
Content-Type: message/sipfrag
Content-Length: (...)

SIP/2.0 100 Trying
```

- Request-URI:** Contains the value of the Contact header from the 200 (OK) response to the initial INVITE.
- Via:** Contains the IP address or FQDN of the originating UE.
- From:/To:/Call-ID:** Contain the values previously used to establish the session, including the tag value from the response.
- Cseq:** Next higher sequential value.
- Security-Verify:** Contains the security agreement as represented by the received Security-Server header.

15. NOTIFY (P-CSCF to S-CSCF) – see example in table 10.5.2-15

P-CSCF#1 forwards the NOTIFY request to S-CSCF#1.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

Table 10.5.2-15: NOTIFY (P-CSCF to S-CSCF)

```
NOTIFY sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
P-Access-Network-Info:
From:
To:
Call-ID:
Cseq:
Contact:
Subscription-State:
Event:
Content-Type:
Content-Length:

SIP/2.0 100 Trying
```

16. NOTIFY (S-CSCF to S-CSCF) – see example in table 10.5.2-16

S-CSCF#1 forwards the NOTIFY request to S-CSCF#2.

Table 10.5.2-16: NOTIFY (S-CSCF to S-CSCF)

```

NOTIFY sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Contact:
Subscription-State:
Event:
Content-Type:
Content-Length:

SIP/2.0 100 Trying

```

17. NOTIFY (S-CSCF to P-CSCF) – see example in table 10.5.2-17

S-CSCF#2 forwards the NOTIFY request to P-CSCF#2.

Table 10.5.2-17: NOTIFY (S-CSCF to P-CSCF)

```

NOTIFY sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Event:
Contact:
Subscription-State:
Content-Type:
Content-Length:

SIP/2.0 100 Trying

```

18. NOTIFY (P-CSCF to UE) – see example in table 10.5.2-18

P-CSCF#2 forwards the NOTIFY request to UE#2.

Table 10.5.2-18: NOTIFY (P-CSCF to UE)

```

NOTIFY sip:[5555::eee:fff:aaa:bbb]:5088;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.home2.net:5088;comp=sigcomp;branch=z9hG4bK876t12.1, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
From:
To:
Call-ID:
Cseq:
Event:
Contact:
Subscription-State:
Content-Type:
Content-Length:

SIP/2.0 100 Trying

```

19. 200 (OK) (UE to P-CSCF) – see example in table 10.5.2-19

UE#2 acknowledges receipt of the NOTIFY request (18) with a 200 (OK) final response, sent to P-CSCF#2.

Table 10.5.2-19: 200 (OK) (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.home2.net;branch=z9hG4bK876t12.1, SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Content-Length: 0
```

20. 200 (OK) (P-CSCF to S-CSCF) – see example in table 10.5.2-20

P-CSCF#2 forwards the 200 (OK) final response to S-CSCF#2.

Table 10.5.2-20: 200 (OK) (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

21. 200 (OK) (S-CSCF to S-CSCF) – see example in table 10.5.2-21

S-CSCF#2 forwards the 200 (OK) final response to S-CSCF#1.

Table 10.5.2-21: 200 (OK) (S-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

22. 200 (OK) (S-CSCF to P-CSCF) – see example in table 10.5.2-22

S-CSCF#1 forwards the 200 (OK) final response to P-CSCF#1.

Table 10.5.2-22: 200 (OK) (S-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

23. 200 (OK) (P-CSCF to UE) – see example in table 10.5.2-23

P-CSCF#1 forwards the 200 (OK) final response to UE#1.

Table 10.5.2-23: 200 (OK) (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Contact:
Content-Length:
```

24. INVITE (UE to P-CSCF) – see example in table 10.5.2-24

UE#1 initiates an INVITE request based on the Refer-To header URL in the REFER request. The INVITE is sent from the UE to P-CSCF#1.

Table 10.5.2-24: INVITE (UE to P-CSCF)

```
INVITE sip:token(tel:+1-212-555-3333)@scscf2.home2.net;lr;tokenized-by=scscf2.home2.net
SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.home1.net:7531;comp=sigcomp;lr>, <sip:scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <tel:+1-212-555-2222>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-c=8642; port-s=7531
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0_0
m=audio 3456 RTP/AVP 97 3 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 G726-32/8000
a=rtpmap:96 telephone-event
a=maxptime:20
```

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

25. 100 (Trying) (P-CSCF to UE) – see example in table 10.5.2-25

P-CSCF#1 responds to the INVITE request (24) with a 100 (Trying) provisional response.

Table 10.5.2-25: 100 (Trying) (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

26. INVITE (P-CSCF to S-CSCF) – see example in table 10.5.2-26

The P-CSCF adds itself to the Record-Route header and Via header.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

Table 10.5.2-26: INVITE (P-CSCF to S-CSCF)

```
INVITE sip:token(tel:+1-212-555-3333)@scscf2.home2.net;lr;tokenized-by=scscf2.home2.net
SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Record-Route: <sip:pcscf1.home1.net;lr>
Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
P-Access-Network-Info:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Require: precondition
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

27. 100 (Trying) (S-CSCF to P-CSCF) – see example in table 10.5.2-27

S-CSCF#1 responds to the INVITE request (26) with a 100 (Trying) provisional response.

Table 10.5.2-27: 100 (Trying) (S-CSCF to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

28. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias.

29. INVITE (S-CSCF to I-CSCF) – see example in table 10.5.2-29

S-CSCF#1 performs an analysis of the destination address, which is a private URL generated by S-CSCF#2. S-CSCF#1 determines the network operator to whom the destination subscriber belongs. Since (for this example) the forwarding network operator does not desire to keep their internal configuration hidden, S-CSCF#1 forwards the INVITE request directly to I-CSCF#2.

Table 10.5.2-29: INVITE (S-CSCF to I-CSCF)

```

INVITE sip:token(tel:+1-212-555-3333)@scscf2.home2.net;lr;tokenized-by=scscf2.home2.net
SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
      pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
      [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

30. INVITE (I-CSCF to S-CSCF) – see example in table 10.5.2-30

I-CSCF#2 performs an analysis of the destination address, which is a private URL generated by S-CSCF#2. I-CSCF#2 forwards the INVITE request directly to S-CSCF#2.

Table 10.5.2-30: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:token(tel:+1-212-555-3333)@scscf2.home2.net;lr;tokenized-by=scscf2.home2.net
SIP/2.0
Via: SIP/2.0/UDP sip:icscf2_s.home2.net;branch=z9hG4bK221s21.2, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

NOTE 1: The I-CSCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

31. 100 (Trying) (S-CSCF to I-CSCF) – see example in table 10.5.2-31

I-CSCF#2 responds to the INVITE request (29) by sending a 100 (Trying) provisional response to S-CSCF#1.

Table 10.5.2-31: 100 (Trying) (S-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

32. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias.

33. INVITE (S-CSCF to I-CSCF) – see example in table 10.5.2-33

S-CSCF#2 determines the destination address from the private URL contained in the INVITE request. Based on information in that URL, and information saved from step #4 above (implementation decision), S-CSCF#2 verifies the validity of the transfer request, and that it is within a short time delay from the REFER request.

S-CSCF#2 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since (for this example) the forwarding network operator does not desire to keep their internal configuration hidden, S-CSCF#2 forwards the INVITE request directly to I-CSCF#3.

S-CSCF#2 translates the destination TEL URL (+1-212-555-3333) into a SIP URI (sip:user3_public1@home3.net).

Table 10.5.2-33: INVITE (S-CSCF to I-CSCF)

```

INVITE sip:user3_public1@home3.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy: none
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

34. 100 (Trying) (I-CSCF to S-CSCF) – see example in table 10.5.2-34

I-CSCF#3 responds to the INVITE request (33) by sending a 100 (Trying) provisional response to S-CSCF#2.

Table 10.5.2-34: 100 (Trying) (I-CSCF to S-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

35. Location Query

I-CSCF (at the border of the terminating subscriber's network) queries the HSS for current location information. It will send "Cx-location-query" to the HSS to obtain the location information for the destination.

36. Location Response

HSS responds with the address of the current S-CSCF for the terminating subscriber.

37. INVITE (I-CSCF to S-CSCF) – see example in table 10.5.2-37

I-CSCF#3 forwards the INVITE request to the S-CSCF (S-CSCF#3) that will handle the session termination.

Table 10.5.2-37: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user3_public1@home3.net SIP/2.0
Via: SIP/2.0/UDP icscf3_s.home3.net;branch=z9hG4bK83th12.7, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:scscf3.home3.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

NOTE 2: The I-CSCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

38. 100 (Trying) (S-CSCF to I-CSCF) – see example in table 10.5.2-38

S-CSCF#3 responds to the INVITE request (37) with a 100 (Trying) provisional response.

Table 10.5.2-38: 100 (Trying) (S-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf3_s.home3.net;branch=z9hG4bK83th12.7, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

39. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias.

40. INVITE (S-CSCF to P-CSCF) – see example in table 10.5.2-40

S-CSCF#3 remembers (from the registration procedure) the next hop CSCF for this UE. It forwards the INVITE request to P-CSCF#3.

Table 10.5.2-40: INVITE (S-CSCF to P-CSCF)

```

INVITE sip:[5555::aaa:bbb:ccc:fff]:9911;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf3.home3.net;branch=z9hG4bKe3yh1k.v, SIP/2.0/UDP
  icscf3_s.home3.net;branch=z9hG4bK83th12.7, SIP/2.0/UDP
  scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
  icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
  scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 64
Route: <sip:pcscf3.home3.net;lr>
Record-Route: <sip:scscf3.home3.net;lr>, <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
  <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
P-Called-Party-ID: <sip:user3_public1@home3.net>
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

41. 100 (Trying) (P-CSCF to S-CSCF) – see example in table 10.5.2-41

P-CSCF#3 responds to the INVITE request (40) by sending a 100 (Trying) provisional response to S-CSCF#3.

Table 10.5.2-41: 100 (Trying) (P-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf3.home3.net;branch=z9hG4bKe3yh1k.v, SIP/2.0/UDP
    icscf3_s.home3.net;branch=z9hG4bK83th12.7, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

42. INVITE (P-CSCF to UE) – see example in table 10.5.2-42

P-CSCF forwards the INVITE request to the UE.

Table 10.5.2-42: INVITE (P-CSCF to UE)

```
INVITE sip:[5555::aaa:bbb:ccc:fff]:9911;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf3.home3.net:1199;comp=sigcomp;branch=z9hG4bK523r01.2, SIP/2.0/UDP
    scscf3.home3.net;branch=z9hG4bKe3yh1k.v, SIP/2.0/UDP
    icscf3_s.home3.net;branch=z9hG4bK83th12.7, SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 63
Record-Route: <sip:pcscf3.home3.net:1199;lr;comp=sigcomp>, <sip:scscf3.home3.net;lr>,
    <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Called-Party-ID:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Remainder of subclause not shown

PROPOSED CHANGE

17.2.2.1 (MO#1b) Mobile origination, roaming (S-S#2, MT#2 assumed)

Figure 17.2.2.1-1 shows an origination procedure which applies to roaming subscribers when the home network operator desires to keep its internal configuration hidden from the visited network. The UE is located in a visited network, and determines the P-CSCF via the CSCF discovery procedure. During registration, the home network allocates an S-CSCF. The home network advertises an I-CSCF as the entry point from the visited network, who forwards requests to the S-CSCF.

When registration is complete, P-CSCF knows the name/address of the next hop in the signalling path toward the S-CSCF, the I-CSCF. I-CSCF receives information in the request, from which it determines the name/address of the proper S-CSCF.

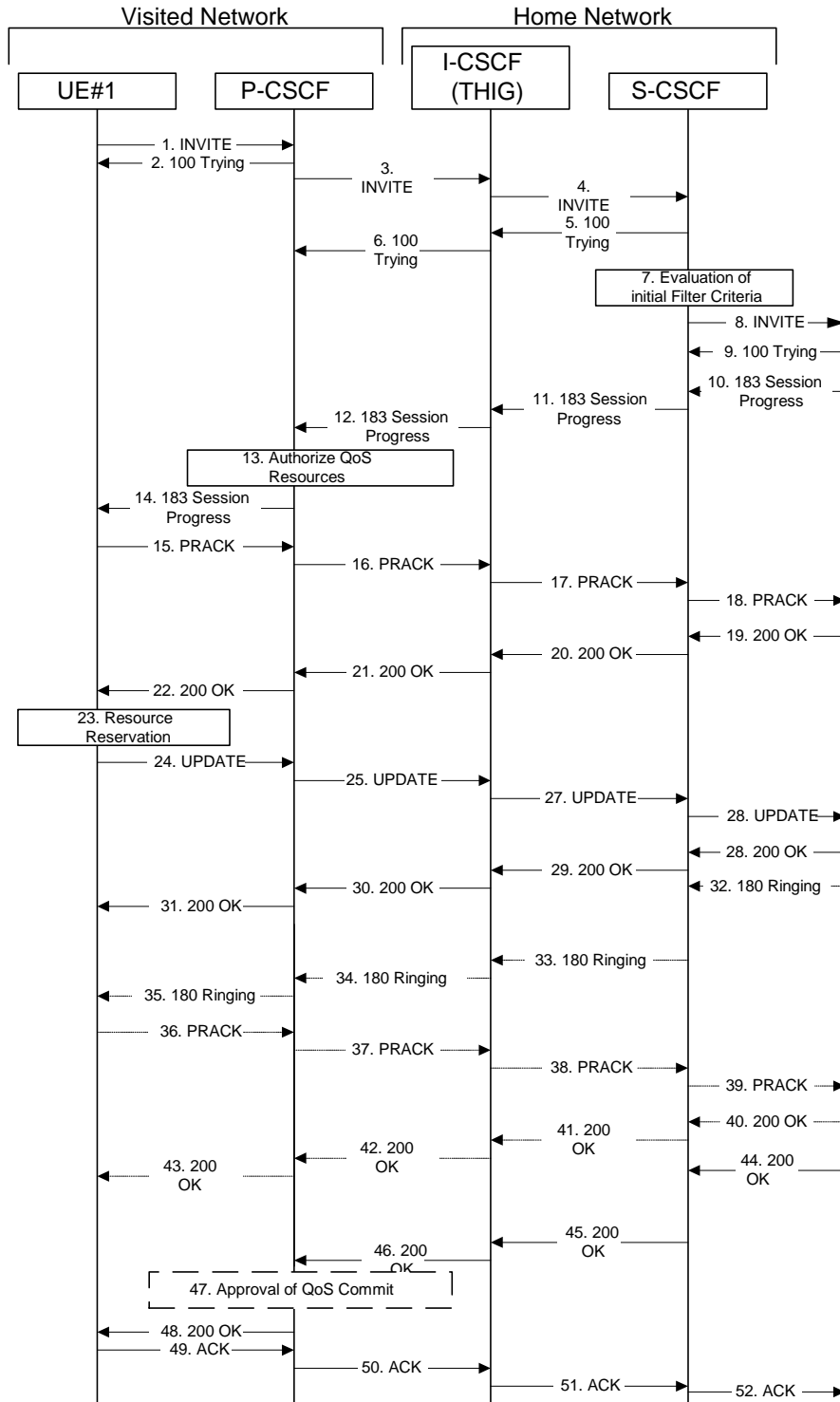


Figure 17.2.2.1-1: MO#1b

Procedure MO#1b is as follows:

1. INVITE (UE to P-CSCF) – see example in table 17.2.2.1-1

UE#1 determines the complete set of codecs that it is capable of supporting for this session. It builds a SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for each possible media flow. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.

For this example, assume UE#1 is capable of sending two simultaneous video streams, either H261 or MPV format, and two simultaneous audio streams, either AMR, G726-32, PCMU, or G728.

UE sends the INVITE request, containing an initial SDP, to the P-CSCF determined via the CSCF discovery mechanism. An example is contained in table 17.2.2.1-1.

Table 17.2.2.1-1: INVITE (UE to P-CSCF)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:icscf1_p.home1.net;lr>,
<sip:Token(sip:scscf1.home1.net;lr)@home1.net;tokenized-by=home1.net>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

Request-URI: Contains the public user identity of the called user.

Via: Contains the IP address or FQDN of the originating UE.

Route: contains the P-CSCF address learnt during P-CSCF discovery, plus the elements from the Service-Route header from registration. The P-CSCF URI contains the port number learnt during the security agreement negotiation

Privacy: the user does not require privacy, therefore the Privacy header is set to the value “none” as specified in RFC 3325 [17] and RFC 3323 [13].

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

P-Preferred-Identity: the user provides a hint about the identity to be used for this session.

Cseq: Is a random starting number.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

Contact: Is a SIP URI that contains the IP address or FQDN of the originating UE.

SDP The SDP contains et of codecs supported by UE#1 and desired by the user at UE#1 for this session

Upon receiving the INVITE, the P-CSCF stores the following information about this session, for use in possible error recovery actions – see example in table 17.2.2.1-1b:

Table 17.2.2.1-1b: Storage of information at P-CSCF

```
Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq(2dest): 127 INVITE
Cseq(2orig): none
Route(2dest): <sip:icscf1_p.home1.net;lr>,
               <sip:Token(sip:scscf1.home1.net;lr)@home1.net;tokenized-by=home1.net>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```

2. 100 Trying (P-CSCF to UE) – see example in table 17.2.2.1-2

P-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 17.2.2.1-2: 100 Trying (P-CSCF to UE)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. INVITE (P-CSCF to I-CSCF) – see example in table 17.2.2.1-3

The P-CSCF adds itself to the Record-Route header and Via header. As the request is forwarded to an interface that is not compressed, the own P-CSCF SIP URI does not contain the "comp=sigcomp" parameter.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

The INVITE request is forwarded through this I-CSCF to the S-CSCF.

Table 17.2.2.1-3: INVITE (P-CSCF to I-CSCF)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:icscf1_p.home1.net;lr>, <sip:Token(sip:scscf1.home1.net;lr)@home1.net;tokenized-
 by=home1.net>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Require: precondition
Supported:
Contact:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Asserted-Identity: The P-CSCF inserts this header based on the user’s hint present in the incoming P-Preferred-Identity header.

P-Charging-Vector: The P-CSCF inserts this header and populates the icid parameters with a globally unique value.

4. INVITE (I-CSCF to S-CSCF) – see example in table 17.2.2.1-4

I-CSCF adds itself to the Record-Route header, and adds a Via header.

I-CSCF determines the routing information contained in the request, and forwards the request to S-CSCF that is serving the UE.

Table 17.2.2.1-4: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:icscf1_p.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity:
P-Access-Network-Info:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Access-Network-Info: This header contains information from the UE.

Upon receiving the INVITE, the S-CSCF stores the following information about this session, for use in possible error recovery actions – see example in table 17.2.2.1-4b:

Table 17.2.2.1-4b: Storage of information at S-CSCF

```

Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): none
Route(2orig): <sip:icscf1_p.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

5. 100 Trying (S-CSCF to I-CSCF) – see example in table 17.2.2.1-5

S-CSCF responds to the INVITE request (4) with a 100 Trying provisional response.

Table 17.2.2.1-5: 100 Trying (S-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscfl_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

6. 100 Trying (I-CSCF to P-CSCF) – see example in table 17.2.2.1-6

I-CSCF forwards the 100 Trying provisional response to P-CSCF.

Table 17.2.2.1-6: 100 Trying (I-CSCF to P-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:

```

7. Evaluation of initial filter criteria

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criteria.

8. INVITE (MO#1b to S-S) – see example in table 17.2.2.1-8

S-CSCF forwards the INVITE request, as specified by the S-CSCF to S-CSCF procedures. As the S-CSCF does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

Table 17.2.2.1-8: INVITE (MO#1b to S-S)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:icscf1_p.home1.net;lr>,
    <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length: (...)

```

```

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Asserted-Identity: The S-CSCF inserts the corresponding TEL URL to the P-Asserted-Identity header in order that the TEL URL is known to the destination network in case the INVITE is forwarded to a MGCF.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the originating Inter Operator Identifier (IOI) parameter of this header.

9. 100 Trying (S-S to MO#1b) – see example in table 17.2.2.1-9 (related to 17.2.2.1-8)

S-CSCF receives a 100 Trying provisional response, as specified by the S-CSCF to S-CSCF procedures.

Table 17.2.2.1-9: 100 Trying (S-S to MO#1b)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```


10. 183 Session Progress (S-S to MO#1b) – see example in table 17.2.2.1-10 (related to 17.2.2.1-8)

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response (to (8)), per the S-CSCF to S-CSCF procedures.

Table 17.2.2.1-10: 183 Session Progress response (S-S to MO#1b)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.home1.net;lr>, <sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:icscf1_p.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Smith" <sip:user2_public1@home1.net>, <tel:+1-212-555-2222>
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
    term-ioi=home2.net
From:
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

Upon receiving the 183 Session Progress, the S-CSCF stores the following information about this session, for use in providing enhanced services, charging or in possible error recovery actions – see example in table 17.2.2.1-10b.

Table 17.2.2.1-10b: Storage of information at S-CSCF

```
Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>; tag=171828
To: <sip:user2_public1@home2.net>; tag=314159
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
Route(2orig): <sip:icscf1_p.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
```


Table 17.2.2.1-15: PRACK (UE to P-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:icscf1_p.home1.net;lr>,
      <sip:Token(<sip:scscf1.home1.net;lr>, <sip:scscf2.home1.net;lr>,
      <sip:pcscf2.home1.net;lr>)>@home1.net;tokenized-by=home1.net>
From: <sip:user1_public1@home1.net>;tag=171828
To:
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 128 PRACK
Require: precondition, sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

- Request-URI:** Takes the value of the Contact header of the received 183 Session Progress response.
- Via:** Take the value of either the IP address of FQDN of the originating UE.
- From:/To:/Call-ID:** Copied from the 183 Session Progress response so that they include any tag parameter.
- Cseq:** Takes a higher value than that in the previous request.
- Security-Verify:** Contains the security agreement as represented by the received Security-Server header.

16. Resource Reservation

After determining the final media streams in step #15, UE initiates the reservation procedures for the resources needed for this session.

17. PRACK (P-CSCF to I-CSCF) – see example in table 17.2.2.1-17

The P-CSCF forwards the PRACK request to the I-CSCF.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

Table 17.2.2.1-17: PRACK (P-CSCF to I-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pscsf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Route: <sip:icscf1_p.home1.net;lr>, <sip:Token(<sip:scscf1.home1.net;lr>,
    <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>@home1.net;tokenized-by=home1.net>
From:
To:
Call-ID:
Cseq:
Require: precondition
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Route: Saved from the Record-Route header of the 183 Session Progress response.

18. PRACK (I-CSCF to S-CSCF) – see example in table 17.2.2.1-18

I-CSCF determines the routing information, and forwards the PRACK request to S-CSCF.

Table 17.2.2.1-19: PRACK (MO#1b to S-S)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

20. 200 OK (S-S to MO#1b) – see example in table 17.2.2.1-20 (related to 17.2.2.1-19)

The destination endpoint responds to the PRACK request (19) with a 200 OK response, per the S-CSCF to S-CSCF procedures.

Table 17.2.2.1-20: 200 OK (S-S to MO#1b)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

21. 200 OK (S-CSCF to I-CSCF) – see example in table 17.2.2.1-21

S-CSCF forwards the 200 OK response to I-CSCF.

Table 17.2.2.1-23: 200 OK (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

24. UPDATE (UE to P-CSCF) – see example in table 17.2.2.1-24

When the resource reservation is completed, UE sends the UPDATE request to the terminating endpoint, via the signalling path established by the INVITE request. The request is sent first to P-CSCF.

Table 17.2.2.1-24: UPDATE (UE to P-CSCF)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:icscf1_p.home1.net;lr>,
      <sip:Token(<sip:scscf1.home1.net;lr>, <sip:scscf2.home1.net;lr>,
      <sip:pcscf2.home1.net;lr>)>@home1.net;tokenized-by=home1.net>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 129 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

- Request-URI:** Takes the value of the Contact header of the received 183 Session Progress response.
- Via:** Take the value of either the IP address or FQDN of the originating UE.
- From:/To:/Call-ID:** Copied from the 183 Session Progress response so that they include any tag parameters.
- Cseq:** Takes a higher value than that in the previous request.
- Security-Verify:** Contains the security agreement as represented by the received Security-Server header.

The SDP indicates that the resource reservation was successful in the local segment.

25. UPDATE (P-CSCF to I-CSCF) – see example in table 17.2.2.1-25

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

The P-CSCF forwards the UPDATE request to the I-CSCF.

Table 17.2.2.1-25: UPDATE (P-CSCF to I-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Route: <sip:icscf1_p.homel.net;lr>, <sip:Token(<sip:scscf1.homel.net;lr>,
    <sip:scscf2.homel.net;lr>, <sip:pcscf2.homel.net;lr>@homel.net;tokenized-by=homel.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024";
    ggsn=[5555::4b4:3c3:2d2:1e1]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-sig=no;
    gcid=A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no; gcid=F312D5E3BC; flow-
    id=({2,1},{2,2})"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

26. UPDATE (I-CSCF to S-CSCF) – see example in table 17.2.2.1-26

I-CSCF determines the routing information, and forwards the request to S-CSCF.

Table 17.2.2.1-27 UPDATE (MO#1b to S-S)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home1.net;lr>, <sip:pcscf2.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

28. 200 OK (S-S to MO#1b) – see example in table 17.2.2.1-28 (related to 17.2.2.1-27)

The destination endpoint responds to the UPDATE request (27) with a 200 OK, per the S-CSCF to S-CSCF procedures.

The SDP indicates that the resource reservation was successful both in the local and the remote segment.

Table 17.2.2.1-28: 200 OK (S-S to MO#1b)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxtime:20

```

29. 200 OK (S-CSCF to I-CSCF) – see example in table 17.2.2.1-29

S-CSCF forwards the 200 OK response to I-CSCF.

Table 17.2.2.1-29 200 OK (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscfl_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscfl.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

30. 200 OK (I-CSCF to P-CSCF) – see example in table 17.2.2.1-30

I-CSCF forwards the 200 OK response to P-CSCF.

Remainder of subclause not shown

PROPOSED CHANGE

17.3.2.1 (S-S#1b) Different network operators performing origination and termination, with configuration hiding by both network operators (MO#2, MT#2 assumed)

Figure 17.3.2.1-1 shows a S-CSCF handling session origination (S-CSCF#1) which performs an analysis of the destination address, and determines that it belongs to a subscriber of a different operator. The originating network operator desires to keep their configuration hidden, so forwards the request through an I-CSCF (I-CSCF#1) to a well-known entry point in the destination operator's network, I-CSCF#2. I-CSCF#2 queries the HSS for current location information, and finds the S-CSCF assigned to the subscriber (S-CSCF#2), and forwards the request to S-CSCF#2. The terminating network operator also desires to keep their configuration hidden, so I-CSCF#2 inserts itself into the signalling path for future exchanges.

Origination sequences that share this common S-CSCF to S-CSCF procedure are:

- MO#1a** Mobile origination, roaming, without a THIG. The "Originating Network" of S-S#1b is therefore a visited network.
- MO#1b** Mobile origination, roaming, with a THIG in home network. The "Originating Network" of S-S#1b is therefore a visited network.
- MO#2** Mobile origination, located in home service area. The "Originating Network" of S-S#1b is therefore the home network.

Termination sequences that share this common S-CSCF to S-CSCF procedure are:

- MT#1a** Mobile termination, roaming, without a THIG. The "Terminating Network" of S-S#1b is a visited network.
- MT#1b** Mobile termination, roaming, with a THIG in home network. The "Terminating Network" of S-S#1b is a visited network.
- MT#2** Mobile termination, located in home service area. The "Terminating Network" of S-S#1b is the home network.

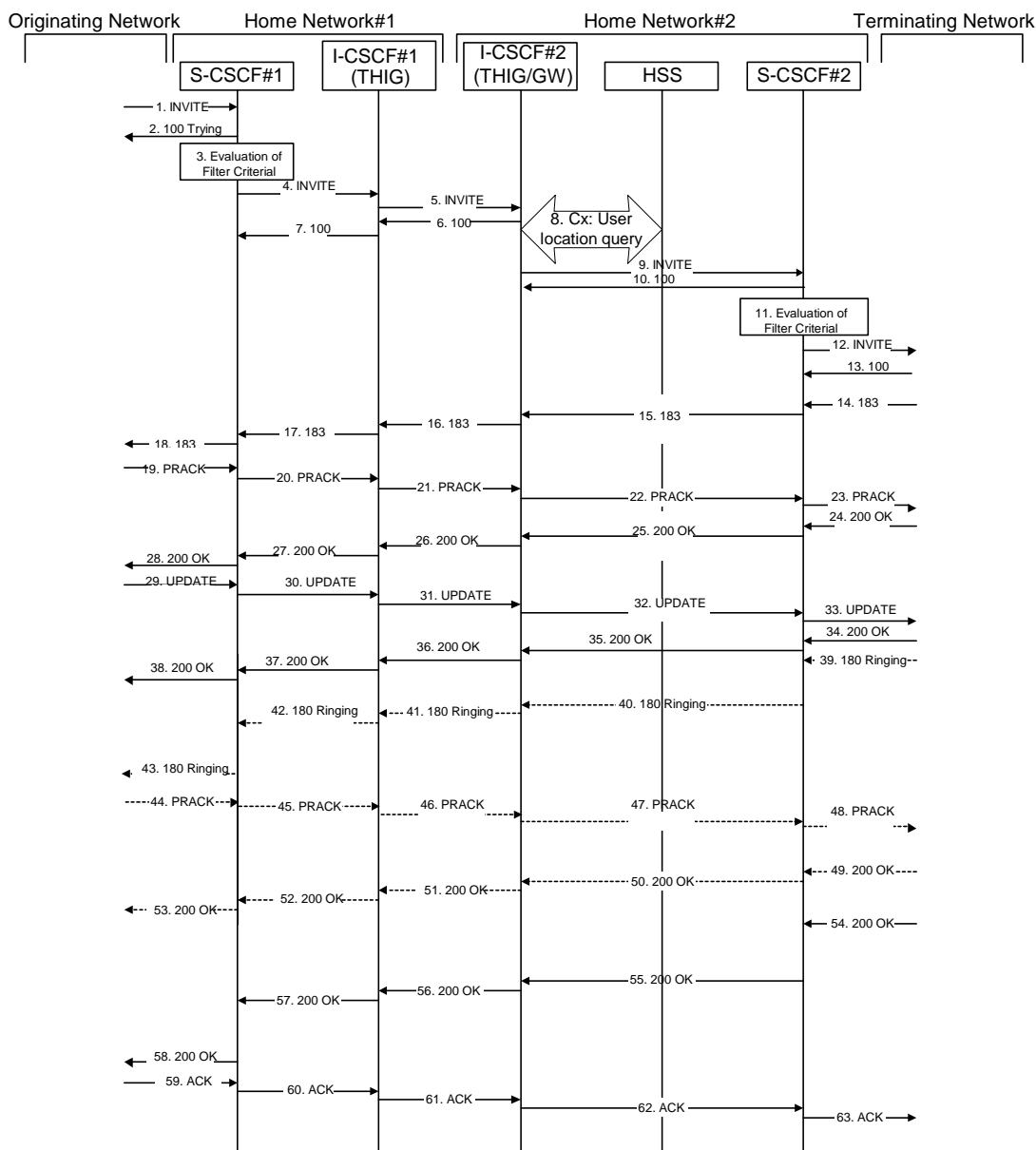


Figure 17.3.2.1-1: S-S#1b

Procedure S-S#1b is as follows:

1. INVITE (MO to S-S#1b) – see example in table 17.3.2.1-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 17.3.2.1-1: INVITE (MO to S-S#1b)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Record-Route: <sip:pcscf1.home1.net;lr>
Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (S-S#1b to MO) – see example in table 17.3.2.1-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 17.3.2.1-2: 100 Trying (S-S#1b to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias. For this example, assume no Application Server involvement.

Table 17.3.2.1-7: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:
```

8. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228 [11].

Table 7.3.2-6a provides the parameters in the SIP INVITE request (flow 5) which are sent to the HSS.

Table 7.3.2-6b provides the parameters sent from the HSS that need to be mapped to the SIP INVITE request (flow 9) and sent to the S-CSCF.

9. INVITE (I-CSCF to S-CSCF) – see example in table 17.3.2.1-9

I-CSCF#2 forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

Table 17.3.2.1-13: 100 Trying (MT to S-S#1b)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

14. 183 Session Progress (MT to S-S#1b) – see example in table 17.3.2.1-14

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response to the INVITE request (12), as per the termination procedure.

Table 17.3.2.1-14: 183 Session Progress (MT to S-S#1b)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.home2.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:icscf2_s.home2.net;lr>, <sip:icscf1_s.home1.net;lr>,
    <sip:Token(<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>)@home1.net;tokenized-
    by=home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
Privacy:
From:
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=crr:qos local none
a=crr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```


Table 17.3.2.1-19: PRACK (MO to S-S#1b)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scsf1.home1.net;lr>, <sip:icsf1_s.home1.net;lr>, <sip:icsf2_s.home2.net;lr>,
 <sip:Token(<sip:scsf2.home2.net;lr>, <sip:pcsf2.home2.net;lr>@home2.net;tokenized-
 by=home2.net)>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 128 PRACK
Require: precondition
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

20. PRACK (S-CSCF to I-CSCF) – see example in table 17.3.2.1-20

S-CSCF#1 forwards the PRACK request to I-CSCF#1.

Table 17.3.2.1-24: 200 OK (MT to S-S#1b)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

25. 200 OK (S-CSCF to I-CSCF) – see example in table 17.3.2.1-25

S-CSCF#2 forwards the 200 OK response to I-CSCF#2.

Table 17.3.2.1-25: 200 OK (S-CSCF to I-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

26. 200 OK (I-CSCF to I-CSCF) – see example in table 17.3.2.1-26

I-CSCF#2 forwards the 200 OK response to I-CSCF#1.

Table 17.3.2.1-27: 200 OK (I-CSCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: I-CSCF#1 decrypts all the tokenised entries belonging to its own network.

28. 200 OK (S-S#1b to MO) – see example in table 17.3.2.1-28

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 17.3.2.1-28: 200 OK (S-S#1b to MO)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

29. UPDATE (MO to S-S#1b) – see example in table 17.3.2.1-29

When the originating endpoint has completed the resource reservation procedures, it sends the UPDATE request to S-CSCF#1 by the origination procedures.

Table 17.3.2.1-29: UPDATE (MO to S-S#1b)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
<sip:Token(<sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>@home2.net;tokenized-
by=home2.net>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

30. UPDATE (S-CSCF to I-CSCF) – see example in table 17.3.2.1-30

S-CSCF#1 forwards the UPDATE request to I-CSCF#1.

Table 17.3.2.1-30: UPDATE (S-CSCF to I-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:icscf1_s.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
<sip:Token(<sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>@home2.net;tokenized-
by=home2.net)>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

31. UPDATE (I-CSCF to I-CSCF) – see example in table 17.3.2.1-31

I-CSCF#1 forwards the UPDATE request to I-CSCF#2.

Table 17.3.2.1-31: UPDATE (I-CSCF to I-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:icscf2_s.home2.net;lr>, <sip:Token(<sip:scscf2.home2.net;lr>,
<sip:pcscf2.home2.net;lr> )@home2.net;tokenized-by=home2.net>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via:: I-CSCF#1 encrypts all the entries belonging to its own network to maintain configuration independence of the home#1 operator.

Table 17.3.2.1-33: UPDATE (S-S#1b to MT)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

34. 200 OK (MT to S-S#1b) – see example in table 17.3.2.1-34

The terminating endpoint responds to the UPDATE request (33) with a 200 OK response.

Table 17.3.2.1-34: 200 OK (MT to S-S#1b)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

35. 200 OK (S-CSCF to I-CSCF) – see example in table 17.3.2.1-35

S-CSCF#2 forwards the 200 OK response to I-CSCF#2.

Table 17.3.2.1-35: 200 OK (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

36. 200 OK (I-CSCF to I-CSCF) – see example in table 17.3.2.1-36

I-CSCF#2 forwards the 200 OK response to I-CSCF#1.

Table 17.3.2.1-36: 200 OK (I-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

37. 200 OK (I-CSCF to S-CSCF) – see example in table 17.3.2.1-37

I-CSCF#1 forwards the 200 OK response to S-CSCF#1.

Table 17.3.2.1-37: 200 OK (I-CSCF to S-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: I-CSCF#1 decrypts all the tokenised entries belonging to its own network.

38. 200 OK (S-S#1b to MO) – see example in table 17.3.2.1-38

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 17.3.2.1-38: 200 OK (S-S#1b to MO)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Remainder of subclause not shown

PROPOSED CHANGE

17.3.3.1 (S-S#1c) Different network operators performing origination and termination, with configuration hiding by originating network operator (MO#2, MT#2 assumed)

Figure 17.3.3.1-1 shows a S-CSCF handling session origination (S-CSCF#1) which performs an analysis of the destination address, and determines that it belongs to a subscriber of a different operator. The originating network operator desires to keep their configuration hidden, so forwards the request through an I-CSCF (I-CSCF#1) to a well-known entry point in the destination operator's network, I-CSCF#2. I-CSCF#2 queries the HSS for current location information, and finds the S-CSCF assigned to the subscriber (S-CSCF#2), and forwards the request to S-CSCF#2. The terminating network operator does not desire to keep their configuration hidden, so I-CSCF#2 does not insert itself into the signalling path for future exchanges.

Origination sequences that share this common S-CSCF to S-CSCF procedure are:

- MO#1a** Mobile origination, roaming, without a THIG. The "Originating Network" of S-S#1c is therefore a visited network.
- MO#1b** Mobile origination, roaming, with a THIG in home network. The "Originating Network" of S-S#1c is therefore a visited network.
- MO#2** Mobile origination, located in home service area. The "Originating Network" of S-S#1c is therefore the home network.

Termination sequences that share this common S-CSCF to S-CSCF procedure are:

- MT#1a** Mobile termination, roaming, without a THIG. The "Terminating Network" of S-S#1c is a visited network.

- MT#1b** Mobile termination, roaming, with a THIG in home network. The "Terminating Network" of S-S#1c is a visited network.
- MT#2** Mobile termination, located in home service area. The "Terminating Network" of S-S#1c is the home network.

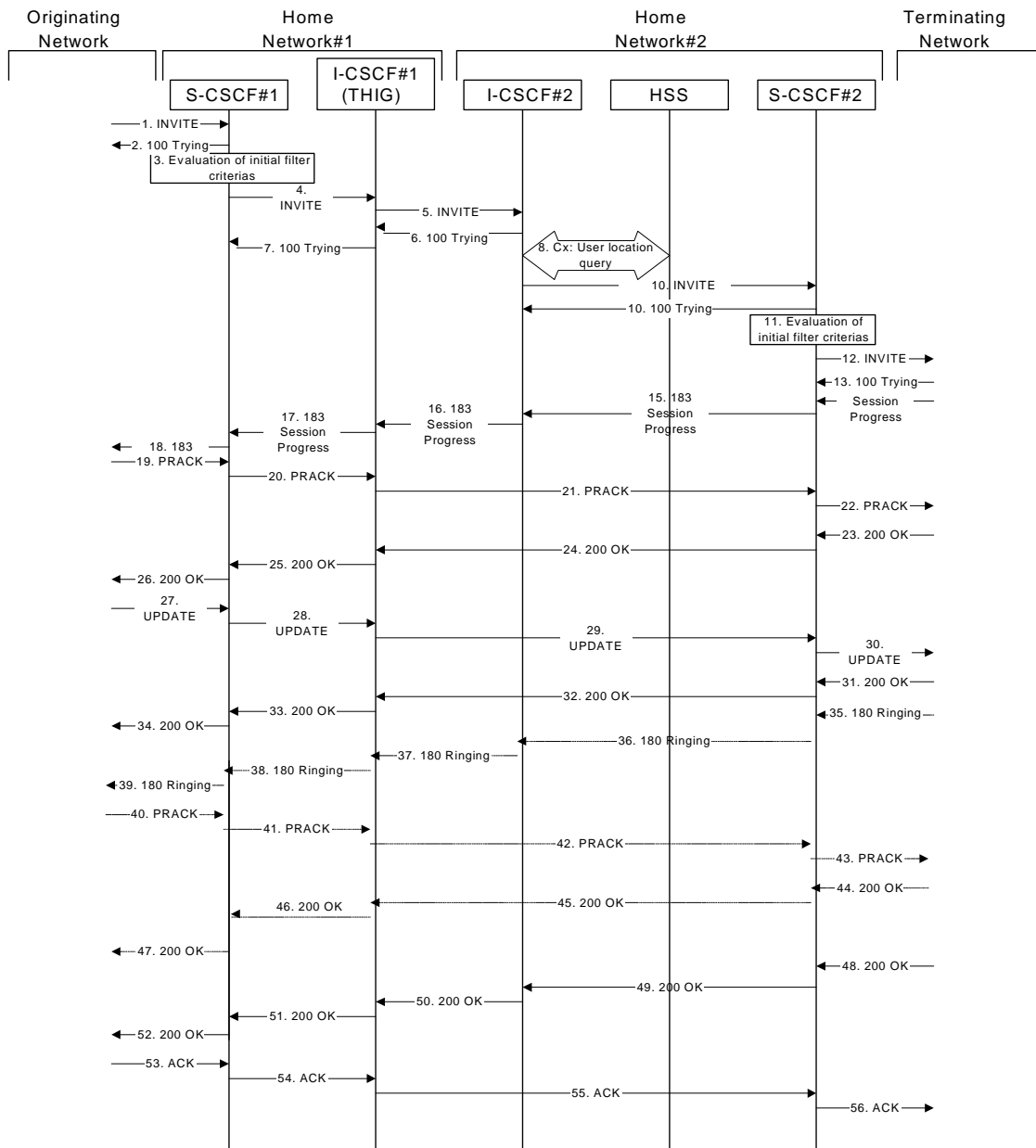


Figure 17.3.3.1-1: S-S#1c

Procedure S-S#1c is as follows:

1. INVITE (MO to S-S#1c) – see example in table 17.3.3.1-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 17.3.3.1-1: INVITE (MO to S-S#1c)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAfrbHLso=023551024"
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (S-S#1c to MO) – see example in table 17.3.3.1-2

S-CSCF#1 responds to the INVITE request (1) with a 100 Trying provisional response.

Table 17.3.3.1-2: 100 Trying (S-S#1c to MO)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of Filter Criteria

S-CSCF#1 validates the service profile of this subscriber, and evaluates the initial filter criterias.

4. INVITE (S-CSCF to I-CSCF) – see example in table 17.3.3.1-4

S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since the originating operator desires to keep their internal configuration hidden, S-CSCF#1 forwards the INVITE request to I-CSCF#1.

Table 17.3.3.1-4: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:icscf1_s.home1.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAfrbHLso=023551024"; orig-ioi=home1.net
From:
To:
Call-ID:
Cseq:
Required:
Supported:
Contact:
Content-Type:
Content-Length: (...)
```

```
v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

Route: Topmost Route header set to the I-CSCF that will perform the translation needed to maintain configuration independence.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the originating Inter Operator Identifier (IOI) parameter of this header.

5. INVITE (I-CSCF to I-CSCF) – see example in table 17.3.3.1-5

I-CSCF#1 finds the entry point in home2.net and forwards the INVITE request to I-CSCF#2.

Table 17.3.3.1-5: INVITE (I-CSCF to I-CSCF)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-
by=home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:Token(<sip:scscf1.home1.net;lr>,
<sip:pcscf1.home1.net;lr>@home1.net;tokenized-by=home1.net>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Via/Record-Route: Translated to maintain configuration independence of the home#1 operator.

6. 100 Trying (I-CSCF to I-CSCF) – see example in table 17.3.3.1-6

I-CSCF#2 responds to the INVITE request (5) with a 100 Trying provisional response.

Table 17.3.3.1-6: 100 Trying (I-CSCF to I-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-
by=home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

7. 100 Trying (I-CSCF to S-CSCF) – see example in table 17.3.3.1-7

I-CSCF#1 determines the Via header, and forwards the 100 Trying provisional response to S-CSCF#1.

Table 17.3.3.1-7: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:
```

8. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228.

Table 7.3.2-6a provides the parameters in the SIP INVITE request (flow 5), which are sent to the HSS.

Table 7.3.2-6b provides the parameters sent from the HSS that are mapped to the SIP INVITE request (flow 9) and sent to the S-CSCF.

9. INVITE (I-CSCF to S-CSCF) – see example in table 17.3.3.1-9

I-CSCF#2 forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

Table 17.3.3.1-9: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:scscf2.home2.net;lr>
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Required:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

10. 100 Trying (S-CSCF to I-CSCF) – see example in table 17.3.3.1-10

S-CSCF#2 responds to the INVITE request with a 100 Trying provisional response.

Table 17.3.3.1-10: 100 Trying (S-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

11. Evaluation of initial filter criteria

S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criterias.t

12. INVITE (S-S#1c to MT) – see example in table 17.3.3.1-12

S-CSCF#2 forwards the INVITE request, as determined by the termination procedure. S-CSCF#2 remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE.

Table 17.3.3.1-12: INVITE (S-S#1c to MT)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
   SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
   SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:pcscf2.home2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:icscf1_s.home1.net;lr>,
   <sip:Token(<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>)@home1.net;tokenized-
   by=home1.net>
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAfrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Required:
Supported:
Contact:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

13.100 Trying (MT to S-S#1c) – see example in table 17.3.3.1-13

S-CSCF#2 receives a 100 Trying provisional response to the INVITE request, as specified by the termination procedures.

Table 17.3.3.1-13: 100 Trying (MT to S-S#1c)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
   SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
   SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

14. 183 Session Progress (MT to S-S#1c) – see example in table 17.3.3.1-14 (related to 17.3.3.1-12)

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response to the INVITE request, as per the termination procedure.

Table 17.3.3.1-14: 183 Session Progress (MT to S-S#1c)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.home2.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:icscf1_s.home1.net;lr>, <sip:Token(<sip:scscf1.home1.net;lr>,
    <sip:pcscf1.home1.net;lr>)@home1.net;tokenized-by=home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Asserted-Identity: "John Smith" <sip:user2_public1@home1.net>
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From:
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

15. 183 Session Progress (S-CSCF to I-CSCF) – see example in table 17.3.3.1-15

S-CSCF#2 forwards the 183 Session Progress provisional response to I-CSCF#2.

Table 17.3.3.1-15: 183 Session Progress (S-CSCF to I-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
     SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
     SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home1.net>, <tel:+1-212-555-2222>
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAfrbHLso=023551024"; orig-ioi=home1.net;
     term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
     ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the terminating Inter Operator Identifier (IOI) parameter of this header.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

16. 183 Session Progress (I-CSCF to I-CSCF) – see example in table 17.3.3.1-16

I-CSCF#2 forwards the 183 Session Progress provisional response to I-CSCF#1.

Table 17.3.3.1-16: 183 Session Progress (I-CSCF to I-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
  scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-
  by=home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

17. 183 Session Progress (I-CSCF to S-CSCF) – see example in table 17.3.3.1-17

I-CSCF#1 forwards the 183 Session Progress provisional response to S-CSCF#1.

Table 17.3.3.1-18: 183 Session Progress (S-S#1c to MO)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

19. PRACK (MO to S-S#1c) – see example in table 17.3.3.1-19

The originator decides the final set of media streams, and includes this information in the PRACK request sent to S-CSCF#1 by the origination procedures.

Table 17.3.3.1-19: PRACK (MO to S-S#1c)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr>, <sip:scscf2.home2.net;lr>,
 <sip:pcscf2.home2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Require: precondition
Cseq: 128 PRACK
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxtime:20

```

20. PRACK (S-CSCF to I-CSCF) – see example in table 17.3.3.1-20

S-CSCF#1 forwards the PRACK request to I-CSCF#1.

Table 17.3.3.1-20: PRACK (S-CSCF to I-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:icscf1_s.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

21. PRACK (I-CSCF to S-CSCF) – see example in table 17.3.3.1-21

I-CSCF#1 forwards the PRACK request to S-CSCF#2.

Table 17.3.3.1-21: PRACK (I-CSCF to S-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-
by=home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

22. PRACK (S-S#1c to MT) – see example in table 17.3.3.1-22

S-CSCF#2 forwards the PRACK request to the terminating endpoint, as per the termination procedure.

Table 17.3.3.1-22: PRACK (S-S#1c to MT)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
  icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
  SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
  SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

23. 200 OK (MT to S-S#1c) – see example in table 17.3.3.1-23

The terminating endpoint responds to the PRACK request with a 200 OK response.

Table 17.3.3.1-23: 200 OK (MT to S-S#1c)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

24. 200 OK (S-CSCF to I-CSCF) – see example in table 17.3.3.1-24

S-CSCF#2 forwards the 200 OK response to I-CSCF#1.

Table 17.3.3.1-24: 200 OK (S-CSCF to I-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-
by=home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

25. 200 OK (I-CSCF to S-CSCF) – see example in table 17.3.3.1-25

I-CSCF#1 forwards the 200 OK response to S-CSCF#1.

Table 17.3.3.1-25: 200 OK (I-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Via: Determined by I-CSCF#1.

26. 200 OK (S-S#1c to MO) – see example in table 17.3.3.1-26

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 17.3.3.1-26: 200 OK (S-S#1c to MO)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

27. UPDATE (MO to S-S#1c) – see example in table 17.3.3.1-27

When the originating endpoint has completed the resource reservation procedures, it sends the UPDATE request to S-CSCF#1 by the origination procedures.

Table 17.3.3.1-27: UPDATE (MO to S-S#1c)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr>, <sip:scscf2.home2.net;lr>,
<sip:pcscf2.home2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

28. UPDATE (S-CSCF to I-CSCF) – see example in table 17.3.3.1-28

S-CSCF#1 forwards the UPDATE request to I-CSCF#1.

Table 17.3.3.1-28: UPDATE (S-CSCF to I-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:icscf1_s.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

29. UPDATE (I-CSCF to S-CSCF) – see example in table 17.3.3.1-29

I-CSCF#1 forwards the UPDATE request to S-CSCF#2.

Table 17.3.3.1-29: UPDATE (I-CSCF to S-CSCF)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-
by=home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

30. UPDATE (S-S#1c to MT) – see example in table 17.3.3.1-30

S-CSCF#2 forwards the UPDATE request to the terminating endpoint, as per the termination procedure.

Table 17.3.3.1-30: UPDATE (S-S#1c to MT)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
    SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
    SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

31. 200 OK (MT to S-S#1c) – see example in table 17.3.3.1-31

The terminating endpoint responds to the UPDATE request with a 200 OK response.

Table 17.3.3.1-31: 200 OK (MT to S-S#1c)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net,
SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net,
SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

```

v=
o=
s=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
~~u=~~
~~o=~~
~~s=~~
~~t=~~
~~m=~~
~~m=~~
~~m=~~
~~m=~~
~~b=~~
~~a=~~
~~a=~~
~~a=~~
~~m=~~
~~a=~~

32. 200 OK (S-CSCF to I-CSCF) – see example in table 17.3.3.1-32

S-CSCF#2 forwards the 200 OK response to I-CSCF#1.

Table 17.3.3.1-32: 200 OK (S-CSCF to I-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP Token(SIP/2.0/UDP
  scscf1.home1.net, SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-
  by=home1.net, SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

33. 200 OK (I-CSCF to S-CSCF) – see example in table 17.3.3.1-33

I-CSCF#1 forwards the 200 OK response to S-CSCF#1.

Table 17.3.3.1-33: 200 OK (I-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Via: Determined by I-CSCF#1.

34. 200 OK (S-S#1c to MO) – see example in table 17.3.3.1-34

S-CSCF#1 forwards the 200 OK response to the originating endpoint.

Table 17.3.3.1-34: 200 OK (S-S#1c to MO)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Remainder of subclause not shown

PROPOSED CHANGE

17.3.4.1 (S-S#1d) Different network operators performing origination and termination, with configuration hiding by terminating network operator (MO#2, MT#2 assumed)

Figure 17.3.4.1-1 shows a S-CSCF handling session origination (S-CSCF#1) which performs an analysis of the destination address, and determines that it belongs to a subscriber of a different operator. S-CSCF#1 forwards the request to a well-known entry point in the destination operator's network, I-CSCF#2. I-CSCF#2 queries the HSS for current location information, and finds the S-CSCF assigned to the subscriber (S-CSCF#2), and forwards the request to S-CSCF#2. The terminating network operator desires to keep their configuration hidden, so I-CSCF#2 inserts itself into the signalling path for future exchanges.

Origination sequences that share this common S-CSCF to S-CSCF procedure are:

- MO#1a** Mobile origination, roaming, without a THIG. The "Originating Network" of S-S#1d is therefore a visited network.
- MO#1b** Mobile origination, roaming, with a THIG in home network. The "Originating Network" of S-S#1d is therefore a visited network.
- MO#2** Mobile origination, located in home service area. The "Originating Network" of S-S#1d is therefore the home network.

Termination sequences that share this common S-CSCF to S-CSCF procedure are:

- MT#1a** Mobile termination, roaming, without a THIG. The "Terminating Network" of S-S#1d is a visited network.

MT#1b Mobile termination, roaming, with a THIG in home network. The "Terminating Network" of S-S#1d is a visited network.

MT#2 Mobile termination, located in home service area. The "Terminating Network" of S-S#1d is the home network.

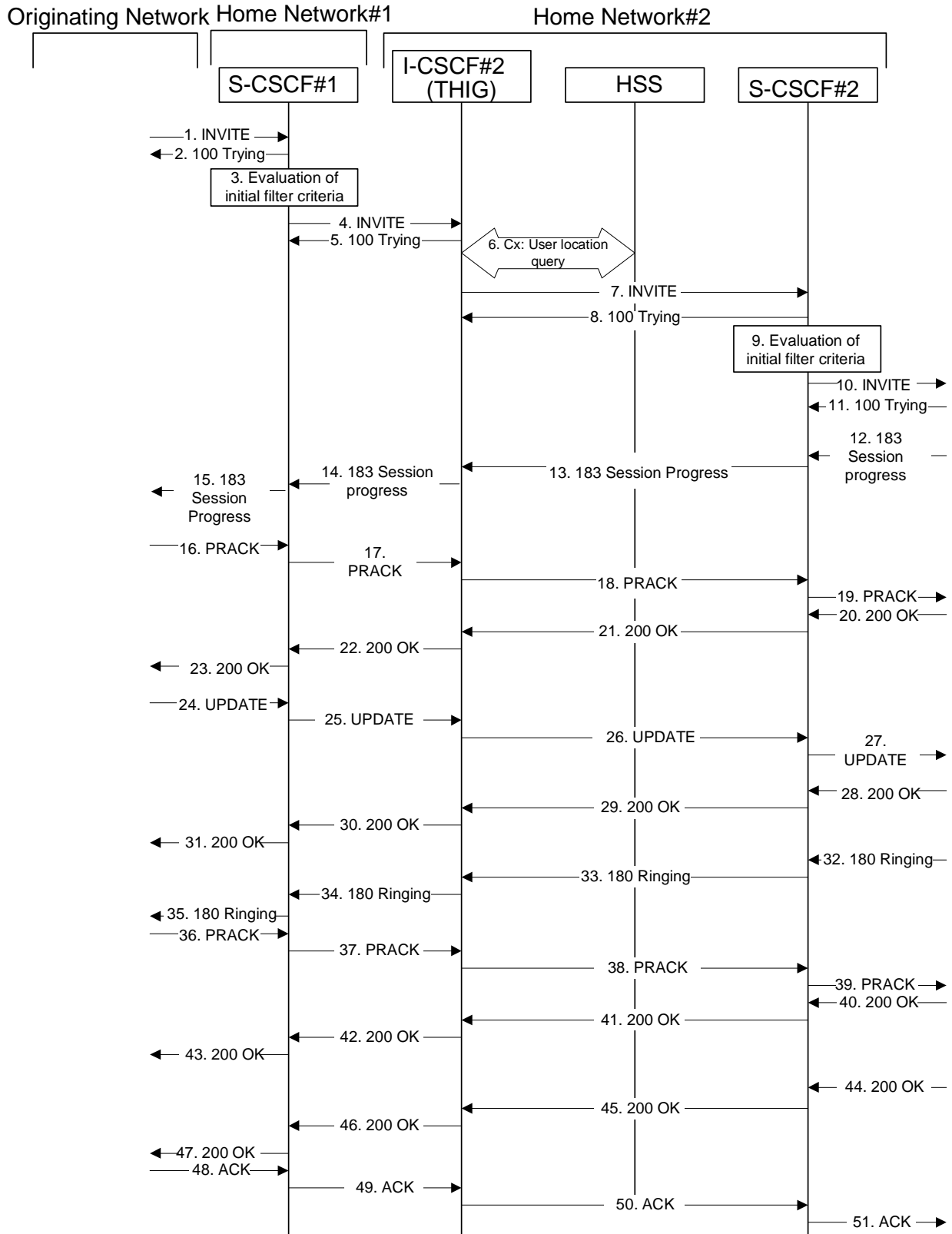


Figure 17.3.4.1-1: S-S#1d

Procedure S-S#1d is as follows:

1. INVITE (MO to S-S#1d) – see example in table 17.3.4.1-1

The INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating signalling flow.

Table 17.3.4.1-1: INVITE (MO to S-S#1d)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <tel:+1-212-555-1111>
Privacy: none
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

2. 100 Trying (S-S#1d to MO) – see example in table 17.3.4.1-2

S-CSCF#1 responds to the INVITE request (1) with a 100 (Trying) provisional response.

Table 17.3.4.1-2: 100 Trying (S-S#1d to MO)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias. For this example, assume no Application Server involvement.

4. INVITE (S-CSCF to I-CSCF) – see example in table 17.3.4.1-4

S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. S-CSCF#1 forwards the INVITE request to I-CSCF#2, the well-known entry point of the destination network.

Table 17.3.4.1-4: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length: (...)
```

```
v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Asserted-Identity: The S-CSCF adds the corresponding TEL URL to the P-Asserted-Identity header in order that the TEL URL is known to the destination network in case the INVITE is forwarded to a MGCF.

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the originating Inter Operator Identifier (IOI) parameter of this header.

5. 100 Trying (I-CSCF to I-CSCF) – see example in table 17.3.4.1-5

I-CSCF#2 responds to the INVITE request (4) with a 100 (Trying) provisional response.

Table 17.3.4.1-5: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228.

Table 7.3.2.1-6a provides the parameters in the SIP INVITE message (flow 4) which need to be sent to HSS.

Table 7.3.2.1-6b provides the parameters sent from the HSS that need to be mapped to SIP INVITE (flow 7) and sent to S-CSCF.

7. INVITE (I-CSCF to S-CSCF) – see example in table 17.3.4.1-7

I-CSCF#2 forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

Table 17.3.4.1-7: INVITE (I-CSCF to S-CSCF)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf1.home2.net;lr>
Record-Route: <sip:icscf2_s.home2.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

8. 100 Trying (S-CSCF to I-CSCF) – see example in table 17.3.4.1-8

S-CSCF#2 responds to the INVITE request (7) with a 100 (Trying) provisional response.

Table 17.3.4.1-8: 100 Trying (S-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

9. Evaluation of initial filter criterias

S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criterias. For this example, assume no Application Server involvement

S-CSCF#2 performs whatever service control logic is appropriate for this session attempt.

10. INVITE (S-S#1d to MT) – see example in table 17.3.4.1-10

S-CSCF#2 forwards the INVITE request, as determined by the termination procedure.

Table 17.3.4.1-10: INVITE (S-S#1d to MT)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
     icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.home2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>,
              <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

11. 100 Trying (MT to S-S#1d) – see example in table 17.3.4.1-11

S-CSCF#2 receives a 100 (Trying) provisional response to the INVITE request (10), as specified by the termination procedures.

Table 17.3.4.1-11: 100 Trying (MT to S-S#1d)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
     icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

12. 183 Session Progress (MT to S-S#1d) – see example in table 17.3.4.1-12

The media stream capabilities of the destination are returned along the signalling path, in a 183 (Session Progress) provisional response to the INVITE request (10), as per the termination procedure.

Table 17.3.4.1-12: 183 Session Progress (MT to S-S#1d)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.home2.net;lr>, <sip:scscf2.home2.net;lr>,
    <sip:icscf2_s.home2.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20
```

13. 183 Session Progress (S-CSCF to I-CSCF) – see example in table 17.3.4.1-13

S-CSCF#2 forwards the 183 (Session Progress) provisional response to I-CSCF#2.

Table 17.3.4.1-13: 183 Session Progress (S-CSCF to I-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKdashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+602IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
    term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
    ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Charging-Vector: The S-CSCF adds the identifier of its own network to the terminating Inter Operator Identifier (IOI) parameter of this header.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

14. 183 Session Progress (I-CSCF to S-CSCF) – see example in table 17.3.4.1-14

I-CSCF#2 forwards the 183 (Session Progress) provisional response to S-CSCF#1.

Table 17.3.4.1-14: 183 Session Progress (I-CSCF to S-CSCF)


```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscfl.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

16. PRACK (MO to S-S#1d) – see example in table 17.3.4.1-16

The originator decides the final set of media streams, and includes this information in the PRACK request sent to S-CSCF#1 by the origination procedures.

Table 17.3.4.1-16: PRACK (MO to S-S#1d)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
 [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scsf1.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
 <sip:token(<sip:pcscf2.home2.net;lr>, <sip:scsf2.home2.net;lr> )@home2.net;tokenized-
 by=home2.net>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 128 PRACK
Require: precondition
RACK: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

17. PRACK (S-CSCF to I-CSCF) – see example in table 17.3.4.1-17

S-CSCF#1 forwards the PRACK request to I-CSCF#2.

Table 17.3.4.1-17: PRACK (S-CSCF to I-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:icscf2_s.home2.net;lr>, <sip:token(<sip:pcscf2.home2.net;lr>,
    <sip:scscf2.home2.net;lr>@home2.net;tokenized-by=home2.net)>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

```

```

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

18. PRACK (I-CSCF to S-CSCF) – see example in table 17.3.4.1-18

I-CSCF#2 determines the routing information, and forwards the PRACK request to S-CSCF#2.

Table 17.3.4.1-18: PRACK (I-CSCF to S-CSCF)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

19. PRACK (S-S#1d to MT) – see example in table 17.3.4.1-19

S-CSCF#2 forwards the PRACK request to the terminating endpoint, as per the termination procedure.

Table 17.3.4.1-19: PRACK (S-S#1d to MT)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

20. 200 OK (MT to S-S#1d) – see example in table 17.3.4.1-20

The terminating endpoint responds to the PRACK request (19) with a 200 (OK) response.

Table 17.3.4.1-20: 200 OK (MT to S-S#1d)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

21. 200 OK (S-CSCF to I-CSCF) – see example in table 17.3.4.1-21

S-CSCF#2 forwards the 200 (OK) response to I-CSCF#2.

Table 17.3.4.1-21: 200 OK (S-CSCF to I-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

22. 200 OK (I-CSCF to S-CSCF) – see example in table 17.3.4.1-22

I-CSCF#2 forwards the 200 (OK) response to S-CSCF#1.

Table 17.3.4.1-22: 200 OK (I-CSCF to S-CSCF)


```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

23. 200 OK (S-S#1d to MO) – see example in table 17.3.4.1-23

S-CSCF#1 forwards the 200 (OK) response to the originating endpoint.

Table 17.3.4.1-23: 200 OK (S-S#1d to MO)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

24. UPDATE (MO to S-S#1d) – see example in table 17.3.4.1-24

When the originating endpoint has completed the resource reservation procedures, it sends the UPDATE request to S-CSCF#1 by the origination procedures.

Table 17.3.4.1-24: UPDATE (MO to S-S#1d)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:scsf1.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
    <sip:token(<sip:pcscf2.home2.net;lr>, <sip:scscf2.home2.net;lr> )@home2.net;tokenized-
    by=home2.net>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

25. UPDATE (S-CSCF to I-CSCF) – see example in table 17.3.4.1-25

S-CSCF#1 forwards the UPDATE request to I-CSCF#2.

Table 17.3.4.1-25: UPDATE (S-CSCF to I-CSCF)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:icscf2_s.home2.net;lr>, <sip:token(<sip:pcscf2.home2.net;lr>,
    <sip:scscf2.home2.net;lr>)>@home2.net;tokenized-by=home2.net>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

26. UPDATE (I-CSCF to S-CSCF) – see example in table 17.3.4.1-26

I-CSCF#2 forwards the UPDATE request to S-CSCF#2.

Table 17.3.4.1-26: UPDATE (I-CSCF to S-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

27. UPDATE (S-S#1d to MT) – see example in table 17.3.4.1-27

S-CSCF#2 forwards the UPDATE request to the terminating endpoint, as per the termination procedure.

Table 17.3.4.1-27: UPDATE (S-S#1d to MT)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

28. 200 OK (MT to S-S#1d) – see example in table 17.3.4.1-28

The terminating endpoint responds to the UPDATE request (27) with a 200 (OK) response.

Table 17.3.4.1-28: 200 OK (MT to S-S#1d)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtmap:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtmap:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

29. 200 OK (S-CSCF to I-CSCF) – see example in table 17.3.4.1-29

S-CSCF#2 forwards the 200 (OK) response to I-CSCF#2.

Table 17.3.4.1-29: 200 OK (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

30. 200 OK (I-CSCF to S-CSCF) – see example in table 17.3.4.1-30

I-CSCF#2 forwards the 200 (OK) response to S-CSCF#1.

Table 17.3.4.1-30: 200 OK (I-CSCF to S-CSCF)


```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

31. 200 OK (S-S#1d to MO) – see example in table 17.3.4.1-31

S-CSCF#1 forwards the 200 (OK) response to the originating endpoint.

Table 17.3.4.1-31: 200 OK (S-S#1d to MO)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Remainder of subclause not shown

PROPOSED CHANGE

17.4.2.1 (MT#1b) Mobile termination, roaming (MO#2, S-S#2 assumed)

Figure 17.4.2.1-1 shows a termination procedure which applies to roaming subscribers when the home network operator desires to keep its internal configuration hidden from the visited network. The UE is located in a visited network, and determines the P-CSCF via the P-CSCF discovery procedure. During registration, the home network allocates a S-CSCF. The home network advertises an I-CSCF as the entry point from the visited network, who protects the S-CSCF identity and forwards requests to the P-CSCF.

When registration is complete, S-CSCF knows the name/address of its next hop in the signalling path toward the UE, the I-CSCF, and the S-CSCF knows the UE Contact address. I-CSCF receives information in the request, which it translates and obtains the name/address of P-CSCF, and P-CSCF obtains the name/address of the UE.

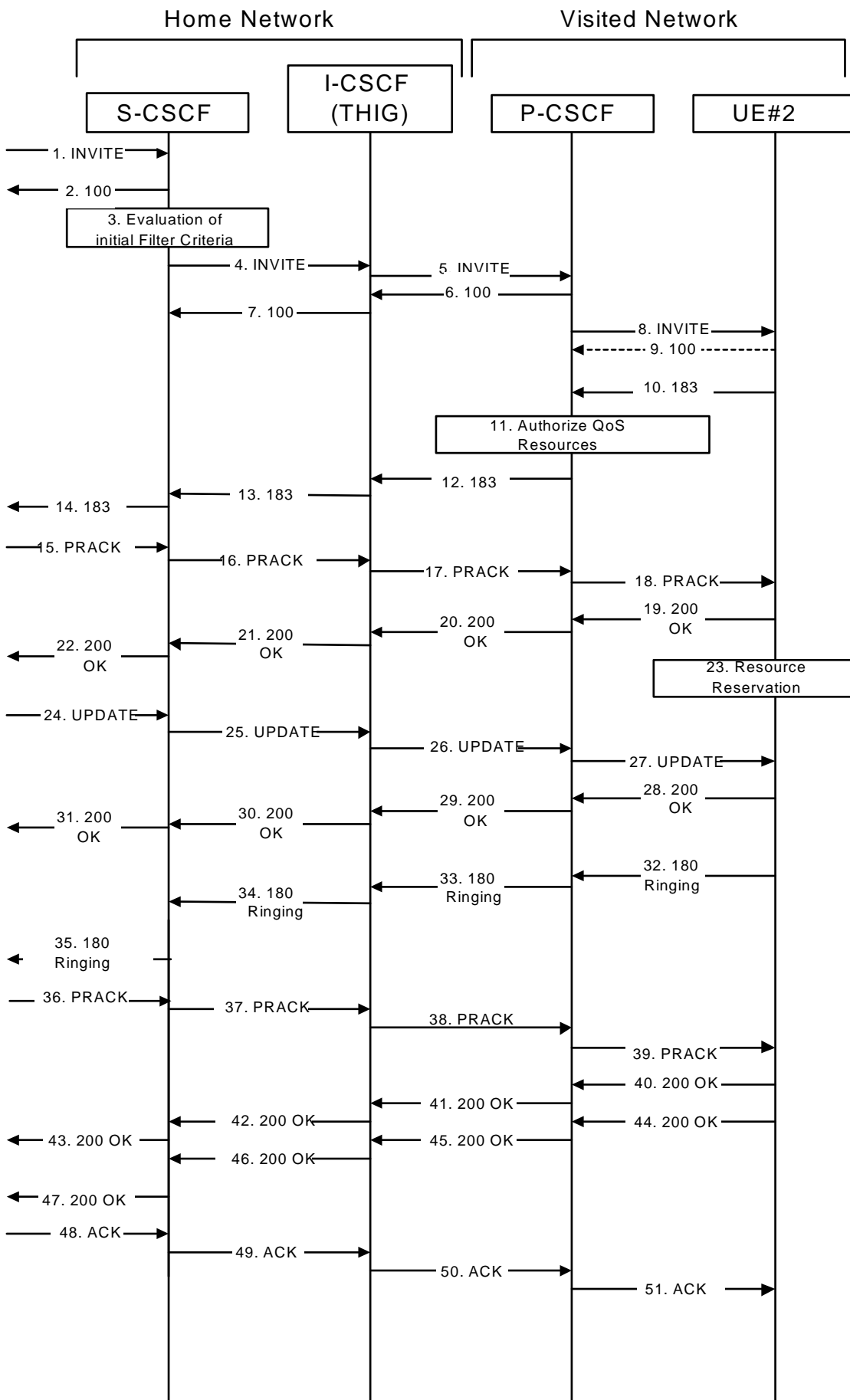


Figure 17.4.2.1-1: MT#1b

Procedure MT#1b is as follows:

1. **INVITE (S-S to MT#1b) – see example in table 17.4.2.1-1**

The calling party sends the INVITE request, via one of the origination procedures and via one of the S-CSCF to S-CSCF procedures, to the S-CSCF for the terminating subscriber.

Table 17.4.2.1-1: INVITE (S-S to MT#1b)

```

INVITE sip:user2_public1@home1.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home1.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: preconditions
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

SDP

The SDP contains the complete set of supported and desired codecs from the session originator.

Upon receipt of the INVITE, the S-CSCF stores the following information about this session, for use in providing enhanced services, charging or in possible error recovery actions – see example in table 17.4.2.1-1b.

Table 17.4.2.1-1b: Storage of information at S-CSCF

```

Request-URI: sip:user2_public1@home1.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
Route(2dest): <sip:icscf2_p.home1.net;lr>, <sip:pcscf2.visited2.net;lr>
Contact(orig): <sip:[5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Contact(dest): <sip:[5555:eee:fff:aaa:bbb]:8805;comp=sigcomp>

```

2. 100 Trying (MT#1b to S-S) – see example in table 17.4.2.1-2

S-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 17.4.2.1-2: 100 Trying (MT#1b to S-S)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criteria

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criteria.

4. INVITE (S-CSCF to I-CSCF) – see example in table 17.4.2.1-4

S-CSCF remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE. It forwards the INVITE to the I-CSCF to perform the THIG functions.

Table 17.4.2.1-4: INVITE (S-CSCF to I-CSCF)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
  icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
  scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:icscf2_p.home1.net;lr>, <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
  ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Via/Record-Route: S-CSCF adds itself in the Record-Route and Via headers.

Request-URI: Built from the registration information.

Route: Built from the Contact address stored at registration.

P-Called-Party-ID: Includes the dialled URL with its parameters.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

5. INVITE (I-CSCF to P-CSCF) – see example in table 17.4.2.1-5

I-CSCF translates the Via headers in the request, and forwards the INVITE request to P-CSCF.

Table 17.4.2.1-5: INVITE (I-CSCF to P-CSCF)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:icscf2_p.home1.net;lr>, <sip:Token(<sip:scscf2.home1.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>)@home1.net;tokenized-by=home1.net>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
P-Called-Party-ID:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: Translated to preserve configuration independence of the home network.

Record-Route: Translated to preserve configuration independence of the home network.

P CSCF saves information from the received INVITE request. The saved value of the information for this session is – see example in table 17.4.2.1-5b:

Table 17.4.2.1-5b: Storage of information at P-CSCF

```

Request-URI: sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfg1kj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:icscf2_p.home1.net;lr>, <sip:Token(<sip:scscf2.home1.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>)@home1.net;tokenized-by=home1.net>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

6. **100 Trying (P-CSCF to I-CSCF)** – see example in table 17.4.2.1-6

P-CSCF responds to the INVITE request (5) with a 100 Trying provisional response.

Table 17.4.2.1-6: 100 Trying (P-CSCF to I-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

7. 100 Trying (I-CSCF to S-CSCF) – see example in table 17.4.2.1-7

I-CSCF determines the Via header, and forwards the 100 Trying provisional response to S-CSCF.

Table 17.4.2.1-7: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:
```

8. INVITE (P-CSCF to UE) – see example in table 17.4.2.1-8

P-CSCF removes the Record-Route and Via headers, calculates the proper Route header to add to future requests, and saves that information without passing it to UE.

Table 17.4.2.1-8: INVITE (P-CSCF to UE)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsfcf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k2l.1, SIP/2.0/UDP
    icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcsfcf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 64
Record-Route: <sip:pcsfcf2.visited2.net:5088;lr;comp=sigcomp>, <sip:icscf2_p.home1.net;lr>,
    <sip:Token(<sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>,
    <sip:pcsfcf1.home1.net;lr>)@home1.net;tokenized-by=home1.net>
P-Media-Authorization:
    0020000100100101706466322e76697369746564322e6e6574000c020133315331343363231
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
P-Called-Party-ID:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its Via header.

Record-Route: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its own URI.

P-Media-Authorization: A P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf2.visited2.net" with credentials "31S14621".

9. 100 Trying (UE to P-CSCF) – see example in table 17.4.2.1-9

UE may optionally send a 100 Trying provisional response to P-CSCF.

Table 17.4.2.1-9: 100 Trying (UE to P-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
    icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

10. 183 Session Progress (UE to P-CSCF) – see example in table 17.4.2.1-10

UE#2 determines the complete set of codecs that it is capable of supporting for this session. It determines the intersection with those appearing in the SDP in the INVITE request. For each media flow that is not supported, UE#2 inserts a SDP entry for media (m= line) with port=0.

UE responds with a 183 Session Progress response containing SDP back to the originator. This SDP may represent one or more media for a multimedia session. This response is sent to P-CSCF.

Table 17.4.2.1-10: 183 Session Progress (UE to P-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscaf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:icscf2_p.home1.net;lr>,
<sip:Token(<sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.home1.net;lr>)@home1.net;tokenized-by=home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From:
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
RSeq: 9021
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98 99
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
a=rtpmap:99 MP4V-ES
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

P-Access-Network-Info: The UE provides the access-type and access-info, related to the serving access network.

To: A tag is added to the To header.

Contact: Identifies the IP address or FQDN of the UE. It includes the comp=sigcomp parameter.

SDP The SDP contains the subset of codecs supported by UE. It requests a confirmation of the QoS preconditions for establishing the session

P-CSCF saves information from the received INVITE request. The saved value of the information for this session is – see example in table 17.4.2.1-10b.

Table 17.4.2.1-10b: Storage of information at P-CSCF

```

Request-URI: sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2orig): <sip:icscf2_p.home1.net;lr>, <sip:Token(<sip:scscf2.home1.net;lr>,
<sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>@home1.net;tokenized-
by=home1.net>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

11. Authorize QoS Resources

P-CSCF authorizes the resources necessary for this session.

12. 183 Session Progress (P-CSCF to I-CSCF) – see example in table 17.4.2.1-12

P-CSCF forwards the 183 Session Progress response to I-CSCF.

Table 17.4.2.1-12: 183 Session Progress (P-CSCF to I-CSCF)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net, SIP/2.0/UDP icscf2_s.home1.net, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:icscf2_p.home1.net;lr>,
<sip:Token(<sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:pcscf1.home1.net;lr>@home1.net;tokenized-by=home1.net>
P-Access-Network-Info:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Record-Route: The P-CSCF rewrites the Record-Route header field value to remove the port number used for the security association and the comp=sigcomp parameter from its own URI

P-Asserted-Identity: P-CSCF inserts the default SIP URI of the user in the P-Asserted-Identity header field.

13. 183-Session-Progress (I-CSCF to S-CSCF) – see example in table 17.4.2.1-13

I-CSCF determines the Via and Record-Route headers, and forwards the response to S-CSCF.

Table 17.4.2.1-13: 183 Session Progress (I-CSCF to S-CSCF)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
     icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
     [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKknashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:icscf2_p.home1.net;lr>,
             <sip:Token(<sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>,
             <sip:pcscf1.home1.net;lr>)>@home1.net;tokenized-by=home1.net>
P-Access-Network-Info:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Access-Network-Info: This header contains information from the UE.

Upon receipt of the 183 Session Progress, the S-CSCF stores the following information about this session, for use in providing enhanced services or in possible error recovery actions – see example in table 17.4.2.1-13b.

Table 17.4.2.1-13b: Storage of information at S-CSCF

```

Request-URI: sip:user2_public1@home2.net
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
CSeq(2dest): 127 INVITE
CSeq(2orig): none
Route(2dest): <sip:icscf2_p.home1.net;lr>, <sip:pcscf2.visited2.net;lr>
Route(2orig): <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
Contact(dest): <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Contact(orig): <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>

```

14. 183 Session Progress (MT#1b to S-S) – see example in table 17.4.2.1-14

S-CSCF forwards the 183 Session Progress response to the originator, per the S-CSCF to S-CSCF procedure.

Table 17.4.2.1-14: 183 Session Progress (MT#1b to S-S)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home1.net>, <tel:+1-212-555-2222>
Privacy: none
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
    term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
    ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
Require:
CSeq:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Charging-Vector: The S-CSCF adds its the identifier of its own network to the terminating Inter Operator Identifier (IOI) parameter of this header and puts back the originating IOI parameter.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

15. PRACK (S-S to MT#1b) – see example in table 17.4.2.1-15

The originating endpoint sends a PRACK request containing the final SDP to be used in this session, via the S-CSCF to S-CSCF procedure, to S-CSCF.

Table 17.4.2.1-15: PRACK (S-S to MT#1b)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home1.net;lr>, <sip:icscf2_p.home1.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 128 PRACK
Require: precondition
RAck: 9021 127 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933616 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

16. PRACK (S-CSCF to I-CSCF) – see example in table 17.4.2.1-16

S-CSCF forwards the PRACK request to I-CSCF.

Table 17.4.2.1-16: PRACK (S-CSCF to I-CSCF)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:icscf2_s.home1.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=

```

17. PRACK (I-CSCF to P-CSCF) – see example in table 17.4.2.1-17

I-CSCF translates the Via headers in the PRACK request, and forwards the request to P-CSCF.

Table 17.4.2.1-17: PRACK (I-CSCF to P-CSCF)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Via: Translated to preserve configuration independence of the home network.

18. PRACK (P-CSCF to UE) – see example in table 17.4.2.1-18

P-CSCF forwards the PRACK request to UE.

Table 17.4.2.1-18: PRACK (P-CSCF to UE)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pscsf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
    icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
    scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pscsf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its own entry in the Via header.

19. 200 OK (UE to P-CSCF) – see example in table 17.4.2.1-19

UE acknowledges the PRACK request (18) with a 200 OK response.

Table 17.4.2.1-19: 200 OK (UE to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscaf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.homel.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.homel.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.homel.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.homel.net;branch=z9hG4bK431h23.1)@homel.net;tokenized-by=homel.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933624 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=conf:qos remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

20. 200 OK (P-CSCF to I-CSCF) – see example in table 17.4.2.1-20

P-CSCF forwards the 200 OK response to I-CSCF.

Table 17.4.2.1-20: 200 OK (P-CSCF to I-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: P-CSCF restores the Via headers from saved values, based on the token value in the branch parameter of its Via.

21. 200 OK (I-CSCF to S-CSCF) – see example in table 17.4.2.1-21

I-CSCF determines the Via and Record-Route headers, and forwards the 200 OK response to S-CSCF.

Table 17.4.2.1-21: 200 OK (I-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

22. 200 OK (MT#1b to S-S) – see example in table 17.4.2.1-22

S-CSCF forwards the 200 OK response to the originator, per the S-CSCF to S-CSCF procedure.

Table 17.4.2.1-22: 200 OK (MT#1b to S-S)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

23. Resource Reservation

UE initiates the reservation procedures for the resources needed for this session.

24. UPDATE (S-S to MT#1b) – see example in table 17.4.2.1-24

When the originating endpoint has completed its resource reservation, it sends the UPDATE request to S-CSCF, via the S-CSCF to S-CSCF procedures.

Table 17.4.2.1-24: UPDATE (S-S to MT#1b)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home1.net;lr>, <sip:icscf2_p.home1.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 129 UPDATE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933617 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=video 3400 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:98 H263
a=fmtp:98 profile-level-id=0
m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 telephone-event
a=maxptime:20

```

25. UPDATE (S-CSCF to I-CSCF) – see example in table 17.4.2.1-25

S-CSCF forwards the UPDATE request to I-CSCF.

Table 17.4.2.1-25: UPDATE (S-CSCF to I-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:icscf2_p.home1.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

26. UPDATE (I-CSCF to P-CSCF) – see example in table 17.4.2.1-26

I-CSCF translates the Via headers in the UPDATE request, and forwards the request to P-CSCF.

Table 17.4.2.1-26: UPDATE (I-CSCF to P-CSCF)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: Translated to preserve configuration independence of the home network.

Record-Route: Translated to preserve configuration independence of the home network.

27. UPDATE (P-CSCF to UE) – see example in table 17.4.2.1-27

P-CSCF forwards the UPDATE request to UE.

Table 17.4.2.1-27: UPDATE (P-CSCF to UE)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: The P-CSCF adds the port number negotiated in the security agreement and the comp=sigcomp parameter to its own entry in the Via header.

28. 200 OK (UE to P-CSCF) – see example in table 17.4.2.1-28

UE acknowledges the UPDATE request (27) with a 200 OK response.

Table 17.4.2.1-28: 200 OK (UE to P-CSCF)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscaf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.homel.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.homel.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
scscf1.homel.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
pcscf1.homel.net;branch=z9hG4bK431h23.1)@homel.net;tokenized-by=homel.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-type: application/sdp
Content-Length: (...)

v=0
o=- 2987933623 2987933625 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=video 10001 RTP/AVP 98
b=AS:75
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:98 H263
a=fmtp:98 profile-level-id=0
m=audio 6544 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20

```

29. 200 OK (P-CSCF to I-CSCF) – see example in table 17.4.2.1-29

P-CSCF forwards the 200 OK response to I-CSCF.

Table 17.4.2.1-29: 200 OK (P-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP Token(SIP/2.0/UDP
scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP
pcscf1.home1.net;branch=z9hG4bK431h23.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

30. 200 OK (I-CSCF to S-CSCF) – see example in table 17.4.2.1-30

I-CSCF determines the Via and Record-Route headers, and forwards the 200 OK to S-CSCF

Table 17.4.2.1-30: 200 OK (I-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
```

31. 200 OK (MT#1b to S-S) – see example in table 17.4.2.1-31

S-CSCF forwards the 200 OK response to the originator, per the S-CSCF to S-CSCF procedure.

Table 17.4.2.1-31: 200 OK (MT#1b to S-S)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Remainder of subclause not shown

PROPOSED CHANGE

17.4.5.1 (MT#1d) Mobile termination, roaming, with I-CSCF in home network providing configuration independence, terminating UE is busy, and not able or not willing to answer the call (MO#2, S-S#2 assumed)

Figure 17.4.5.1-1 shows a termination procedure which applies to roaming subscribers when the home network operator desires to keep its internal configuration hidden from the visited network. The UE is located in a visited network, and determines the P-CSCF via the P-CSCF discovery procedure. During registration, the home network allocates the S-CSCF.

When registration is complete, S-CSCF knows the name/address of P-CSCF and the UE Contact address, and P-CSCF obtains the name/address of the UE.

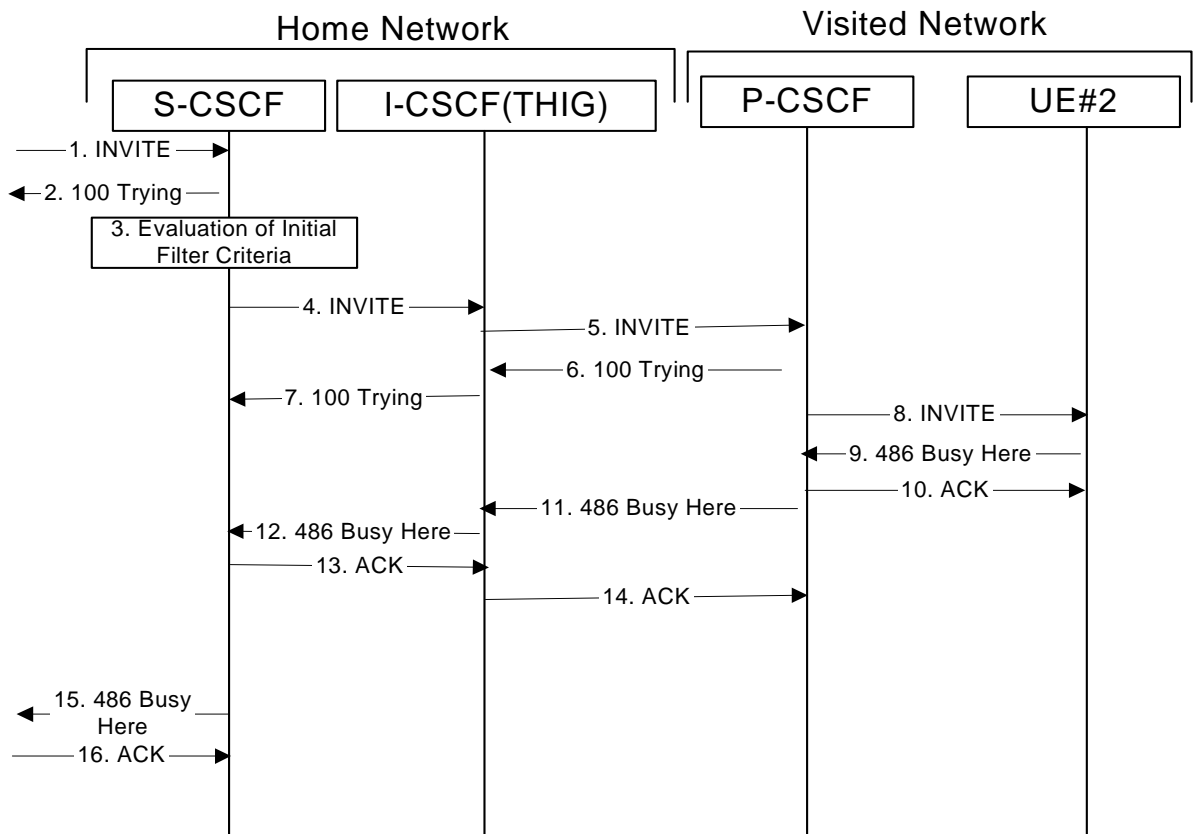


Figure 17.4.5.1-1: MT#1d

Procedure MT#1d is as follows:

1. INVITE (S-S to MT#1d) – see example in table 17.4.5.1-1

The calling party sends the INVITE request, via one of the origination procedures and via one of the S-CSCF to S-CSCF procedures, to the S-CSCF for the terminating subscriber.

Table 17.4.5.1-1: INVITE (S-S to MT#1d)

```

INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Charging-Vector: icid-value="AyretyU0dm+602Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: precondition
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907165275_0_0
m=audio 3456 RTP/AVP 97 3 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtpmap:96 G726-32/8000
a=rtpmap:96 telephone-event
a=maxptime:20

```

2. 100 Trying (MT#1d to S-S) – see example in table 17.4.5.1-2

S-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 17.4.5.1-2: 100 Trying (MT#1d to S-S)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

3. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber, and evaluates the initial filter criterias.

4. INVITE (S-CSCF to I-CSCF) – see example in table 17.4.5.1-4

S-CSCF remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE. It forwards the INVITE to the I-CSCF to perform the THIG functions.

Table 17.4.5.1-4: INVITE (S-CSCF to I-CSCF)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:icscf2_p.home1.net;lr>, <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
    ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
P-Called-Party-ID: <sip:user1_public1@home2.net>
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Route: Built from the Contact address stored at registration.

P-Called-Party-ID: Includes the dialled URL with its parameters.

Via/Record-Route: S-CSCF adds itself in the Record-Route and Via headers.

P-Charging-Function-Addresses: The S-CSCF passes this header to the I-CSCF for charging.

5. INVITE (I-CSCF to P-CSCF) – see example in table 17.4.5.1-5

I-CSCF translates the Via headers in the request, and forwards the INVITE request to P-CSCF.

Table 17.4.5.1-5: INVITE (I-CSCF to P-CSCF)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP
    Token(scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
        icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
        scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
        pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
        [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:icscf2_p.home1.net;lr>, <sip:Token(<sip:scscf2.home1.net;lr>,
    <sip:scscf1.home1.net;lr>), <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Require:
Supported:
P-Called-Party-ID:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Via: Translated to preserve configuration independence of the home network.

Record-Route: Translated to preserve configuration independence of the home network.

6. 100 Trying (P-CSCF to I-CSCF) – see example in table 17.4.5.1-6

P-CSCF responds to the INVITE request (5) with a 100 Trying provisional response.

Table 17.4.5.1-6: 100 Trying (P-CSCF to I-CSCF)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP
    Token(scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
        icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
        scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
        pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
        [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

7. 100 Trying (I-CSCF to S-CSCF) – see example in table 17.4.5.1-7

I-CSCF determines the Via header, and forwards the 100 Trying provisional response to S-CSCF.

Table 17.4.5.1-7: 100 Trying (I-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:
```

8. INVITE (P-CSCF to UE) – see example in table 17.4.5.1-8

P-CSCF forwards the INVITE request to the UE.

Table 17.4.5.1-8: INVITE (P-CSCF to UE)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
    icscf2_p.home1.net;branch=z9hG4bKa9012.1, SIP/2.0/UDP
    Token(scscf2.home1.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home1.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 64
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:icscf2_p.home1.net;lr>,
    <sip:Token(<sip:scscf2.home1.net;lr>, <sip:scscf1.home1.net;lr>)>, <sip:pcscf1.home1.net;lr>
P-Asserted-Identity:
Privacy:
P-Media-Authorization:
    0020000100100101706466322e76697369746564322e6e6574000c020133315331343363231
From:
To:
Call-ID:
Cseq:
Contact:
Require:
Supported:
P-Called-Party-ID:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Media-Authorization: A P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf2.visited2.net" with credentials "31S14621".

Record-Route: The P-CSCF ads the port number negotiated in the security agreement and the comp=sigcomp parameter to its own SIP URI.

Remainder of subclause not shown

PROPOSED CHANGE

17.5.2 Sample multimedia signalling flow - addition of further media originator and terminator are both roaming and operated by different networks

Figure 17.5.2-1 shows a multimedia signalling flow for the addition of another media where the originator and terminator are both roaming and operated by different networks. Both networks are with I-CSCF providing configuration independence. The UE has already established an IM CN session carrying voice and is generating an INVITE request to add video media to the already established IM session.

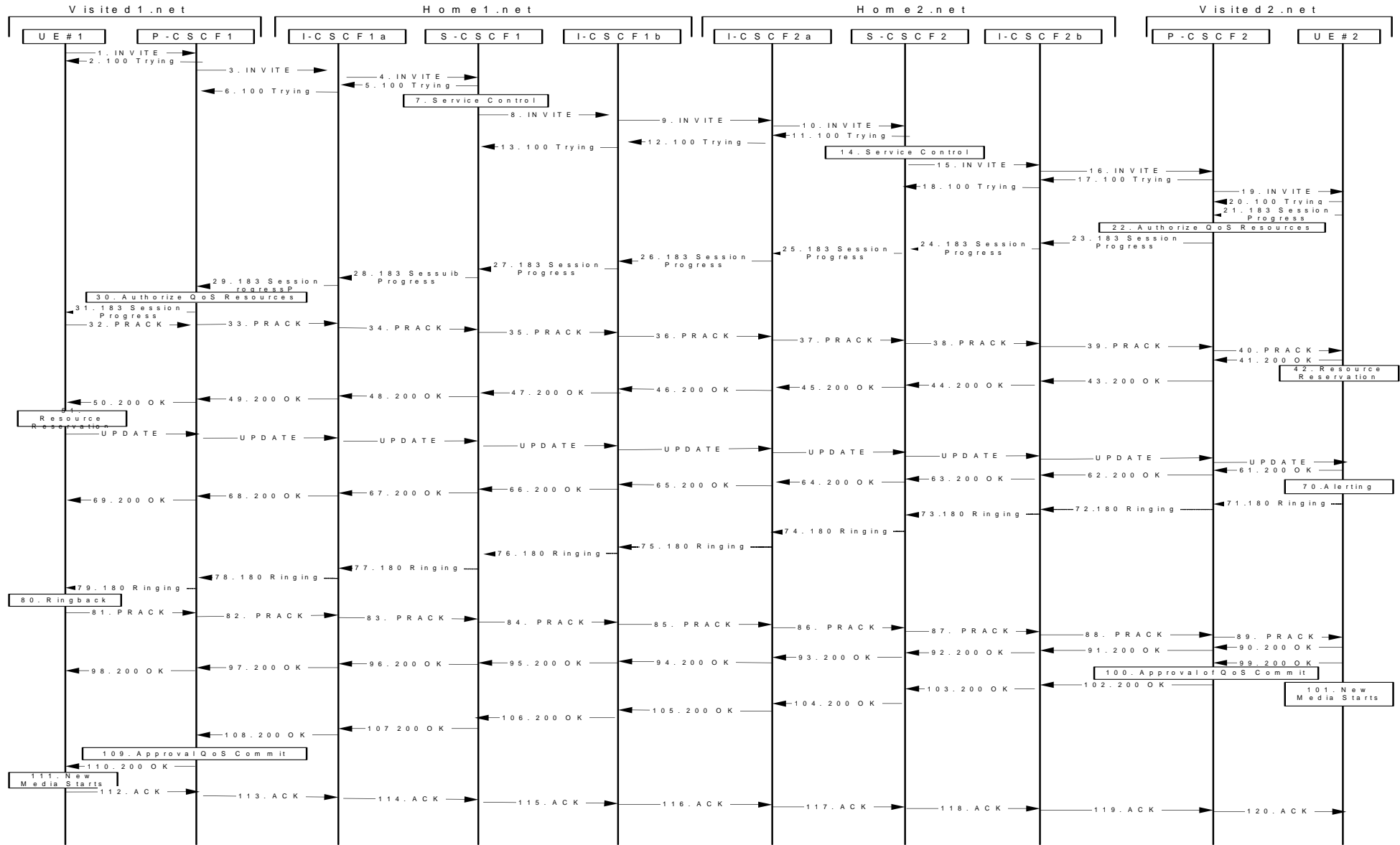


Figure 17.5.2-1: Sample multimedia signalling flow - additional of further media with I-CSCF (THIG)

1. INVITE (UE1 to P-CSCF1) - see example in table 17.5.2-1

UE sends the Re-INVITE request, containing another media description in SDP, to the P-CSCF determined via the CSCF discovery mechanism. An example is contained in table 17.5.2-1.

Table 17.5.2-1: INVITE (UE1 to P-CSCF1)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:icscf1_p.home1.net;lr>,
<sip:token(<sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr> )@home1.net;tokenized-
by=home1.net>, <sip:icscf2_s.home2.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_p.home2.net;lr> )@home2.net;tokenized-by=home2.net>,
<sip:pcscf2.visited2.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
CSeq: 132 INVITE
Require: precondition, sec-agree
Proxy-Require: sec-agree
Supported: 100rel
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907166275-0_0
m=audio 3456 RTP/AVP 97
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=maxptime:20
a=rtptime:96 telephone-event
m=video 9544 RTP/AVP 31
b=AS:54.6
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:31 H261/90000
```

Request-URI: Contains the keyed number from the user. This is specified by the UE as sip:<keyed number>@home1.net. This is in accordance to standard IETF procedure for specifying dialed digits.

Via: Contains the IP address or FQDN of the originating UE.

P-Preferred-Identity: the user provides a hint about the identity to be used for this session.

P-Access-Network-Info: The UE provides the access-type and access-info, related to the serving access network.

From:/To:/Call-ID: Follow the recommendations of RFC 3323 [13], even though anonymity is not being requested for this session.

Cseq: Is a random starting number.

Contact: Is a SIP URI that contains the IP address or FQDN of the originating UE.

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

2. 100 Trying (P-CSCF1 to UE1) - see example in table 17.5.2-2

P-CSCF responds to the INVITE request (1) with a 100 Trying provisional response.

Table 17.5.2-2: 100 Trying (P-CSCF1 to UE1)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

3. INVITE (P-CSCF1 to I-CSCF1a) - see example in table 17.5.2-3

P-CSCF1 forwards the INVITE to the next hop name/address, as determined from previous response messages.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

Table 17.5.2-3: INVITE (P-CSCF1 to I-CSCF1a)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsfc1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Record-Route: <sip:pcsfc1.visited1.net;lr>
Route: <sip:icscf1_p.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
  <sip:icscf1_s.home1.net;lr>@home1.net;tokenized-by=home1.net>,
  <sip:icscf2_s.home2.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
  <sip:icscf2_p.home2.net;lr>@home2.net;tokenized-by=home2.net>,
  <sip:pcsfc2.visited2.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Require: precondition
Supported:
Contact:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

4. INVITE (I-CSCF1a to S-CSCF1) - see example in table 17.5.2-4

I-CSCF1a performs the THIG function and forwards the invite to S-CSCF1.

Table 17.5.2-4: INVITE (I-CSCF1a to S-CSCF1)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:icscf1_p.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
Route: <sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
<sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr>)&#x2D;tokenized-
by=home2.net>, <sip:pcscf2.visited2.net;lr>
P-Asserted-Identity:
P-Access-Network-Info:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

P-Access-Network-Info: This header contains information from the UE.

5. **100 Trying (S-CSCF1 to I-CSCF1a)** - see example in table 17.5.2-5

S-CSCF1 sends the 100 Trying provisional response to P-CSCF1 through I-CSCF1a.

Table 17.5.2-5: 100 Trying (S-CSCF1 to I-CSCF1a)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:

```

6. **100 Trying (I-CSCF1a to P-CSCF1)** - see example in table 17.5.2-6

I-CSCF1a forwards the 100 Trying provisional response to P-CSCF1.

Table 17.5.2-6: 100 Trying (I-CSCF1a to P-CSCF1)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length:

```

7. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber and evaluates the initial filter criterias.

8. INVITE (S-CSCF1 to I-CSCF1b) - see example in table 17.5.2-8

S-CSCF1 recognizes that this invite applies to an existing session. It therefore forwards the INVITE along the existing path to I-CSCF1b.

Table 17.5.2-8: INVITE (S-CSCF1 to I-CSCF1b)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:icscf1_p.home1.net;lr>,
    <sip:pcscf1.visited1.net;lr>
Route: <sip:icscf1_s.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
    <sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr>)&#106;home2.net;tokenized-
    by=home2.net>, <sip:pcscf2.visited2.net;lr>
P-Asserted-Identity: <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"; orig-ioi=home1.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
    ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

9. INVITE (I-CSCF1b to I-CSCF2a) - see example in table 17.5.2-9

I-CSCF1b forwards the INVITE request to the next hop I-CSCF2a and performs the THIG function.

Table 17.5.2-9: INVITE (I-CSCF1b to I-CSCF2a)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Record-Route: <sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>)@home1.net;tokenized-by=home1.net>,
<sip:pcscf1.visited1.net;lr>
Route: <sip:icscf2_s.home2.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_p.home2.net;lr>)@home2.net;tokenized-by=home2.net>,
<sip:pcscf2.visited2.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

10. INVITE (I-CSCF2a to S-CSCF2) - see example in table 17.5.2-10

I-CSCF2a forwards the INVITE request to S-CSCF2.

Table 17.5.2-10: INVITE (I-CSCF2a to S-CSCF2)

```

INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Record-Route: <sip:icscf2_s.home2.net;lr>, <sip:icscf1_s.home1.net;lr>,
    <sip:token(<sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr>)@home1.net;tokenized-
    by=home1.net>, <sip:pcscf1.visited1.net;lr>
Route: <sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

11. 100 Trying (S-CSCF2 to I-CSCF2a) - see example in table 17.5.2-11

S-CSCF2 sends a 100 Trying provisional response back to S-CSCF1 through I-CSCF2a.

Table 17.5.2-11: 100 Trying (S-CSCF2 to I-CSCF2a)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

12. 100 Trying (I-CSCF2a to I-CSCF1b) - see example in table 17.5.2-12

I-CSCF2a forwards a 100 Trying provisional response to the upstream next hop I-CSCF1b.

Table 17.5.2-12: 100 Trying (I-CSCF2a to I-CSCF1b)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

13. 100 Trying (I-CSCF1b to S-CSCF1) - see example in table 17.5.2-13

I-CSCF forwards a 100 Trying provisional response to the S-CSCF1.

Table 17.5.2-13: 100 Trying (I-CSCF1b to S-CSCF1)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

14. Evaluation of initial filter criterias

S-CSCF validates the service profile of this subscriber and evaluates the initial filter criterias.

15. INVITE (S-CSCF2 to I-CSCF2b) - see example in table 17.5.2-15

S-CSCF2 recognizes that this invite applies to an existing session. It therefore forwards the INVITE along the existing path to I-CSCF2b.

Table 17.5.2-15: INVITE (S-CSCF2 to I-CSCF2b)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
  icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
  icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
  scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
  pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKdashds7
Max-Forwards: 64
Record-Route: <sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>,
  <sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
  <sip:icscf1_s.home1.net;lr>@home1.net;tokenized-by=home1.net>,
  <sip:pcscf1.visited1.net;lr>
Route: <sip:icscf2_p.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrHLso=023551024"
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
  ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (...)

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

16. INVITE (I-CSCF2b to P-CSCF2) - see example in table 17.5.2-16

I-CSCF2b performs the THIG function and forwards the INVITE request to P-CSCF2.

Table 17.5.2-16: INVITE (I-CSCF2 to P-CSCF2)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 63
Record-Route: <sip:icscf2_p.home2.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_s.home2.net;lr>)@home2.net;tokenized-by=home2.net>,
<sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>)@home1.net;tokenized-by=home1.net>,
<sip:pcscf1.visited1.net;lr>
Route: <sip:pcscf2.visited2.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
P-Called-Party-ID:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

17.100 Trying (P-CSCF2 to I-CSCF2b) - see example in table 17.5.2-17

P-CSCF2 sends a 100 Trying provisional response back to S-CSCF2 through I-CSCF2b.

Table 17.5.2-17: 100 Trying (P-CSCF2 to I-CSCF2b)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

18. 100 Trying (I-CSCF2b to S-CSCF2) - see example in table 17.5.2-18

I-CSCF2b forwards a 100 Trying provisional response back to S-CSCF2.

Table 17.5.2-18: 100 Trying (I-CSCF2b to S-CSCF2)

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0

```

19. INVITE (P-CSCF2 to UE2) - see example in table 17.5.2-19

P-CSCF forwards the INVITE request to the UE.

Table 17.5.2-19: INVITE (P-CSCF2 to UE2)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
  icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
  scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
  icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
  icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
  scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
  icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
  pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
  [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 62
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:icscf2_p.home2.net;lr>,
  <sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>)@home2.net;tokenized-
  by=home2.net>, <sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
  <sip:icscf1_s.home1.net;lr>)@home1.net;tokenized-by=home1.net>,
  <sip:pcscf1.visited1.net;lr>
P-Media-Authorization:
  0020000100100101706466322e76697369746564322e6e6574000c020133315331343363233
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Supported:
Contact:
P-Called-Party-ID:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Media-Authorization: A P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf2.visited2.net" with credentials "31S14623".

Via: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its Via header.

Record-Route: The P-CSCF adds the port number negotiated during the security agreement and the comp=sigcomp parameter to its own URI.

20.100 Trying (UE2 to P-CSCF2) - see example in table 17.5.2-20

UE2 sends a 100 Trying provisional response back to P-CSCF2.

Table 17.5.2-20: 100 Trying (UE2 to P-CSCF2)

```
SIP/2.0 100 Trying
Via: pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bKert23.8 SIP/2.0/UDP, SIP/2.0/UDP
    icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
    scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

21.183 Session Progress (UE2 to P-CSCF2) - see example in table 17.5.2-21

The media stream capabilities of the destination are returned along the signalling path, in a 183 Session Progress provisional response.

Table 17.5.2-21: 183 Session Progress response (UE2 to P-CSCF2)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscaf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:icscf2_p.home2.net;lr>,
<sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>)@home2.net;tokenized-
by=home2.net>, <sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>)@home1.net;tokenized-by=home1.net>,
<sip:pcscf1.visited1.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From:
To:
Call-ID:
CSeq:
Require: 100rel
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;lr;comp=sigcomp>
RSeq: 9022
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=907166275-0_0
m=audio 6544 RTP/AVP 97
b=AS:25.4 3
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
m=video 7544 RTP/AVP 31
b=AS:54.6
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:31 H261/90000

```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

22. Authorize QoS Resources

P-CSCF2 authorizes the resources necessary for this new media.

23. 183 Session Progress (P-CSCF2 to I-CSCF2b) - see example in table 17.5.2-23

P-CSCF forwards the 183 Session Progress response to P-CSCF.

Table 17.5.2-23: 183 Session Progress (P-CSCF2 to I-CSCF2b)

```

SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:icscf2_p.home2.net;lr>,
<sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>)@home2.net;tokenized-
by=home2.net>, <sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>)@home1.net;tokenized-by=home1.net>,
<sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
P-Access-Network-Info:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrBHLso=023551024"
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

Record-Route: The P-CSCF rewrites the Record-Route header to remove the port number and the comp=sigcomp parameter from its own SIP URI.

24. 183 Session Progress (I-CSCF2b to S-CSCF2) - see example in table 17.5.2-24

I-CSCF2b forwards the 183 Session Progress response to S-CSCF2.

Table 17.5.2-24: 183 Session Progress (I-CSCF2b to S-CSCF2)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:icscf2_p.home2.net;lr>,
    <sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>, <sip:icscf1_s.home1.net;lr>,
    <sip:token(<sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr>)@home1.net;tokenized-
    by=home1.net>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
P-Access-Network-Info:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Access-Network-Info: This header contains information from the UE.

25. 183 Session Progress (S-CSCF2 to I-CSCF2a) - see example in table 17.5.2-25

S-CSCF2 forwards the 183 Session Progress response to I-CSCF2a.

Table 17.5.2-25: 183 Session Progress (S-CSCF2 to I-CSCF2a)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
term-ioi=home2.net
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

26. 183 Session Progress (I-CSCF2a to I-CSCF1b) - see example in table 17.5.2-26

I-CSCF2a forwards the 183 Session Progress response to I-CSCF1b.

Table 17.5.2-26: 183 Session Progress (I-CSCF2a to I-CSCF1b)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net/1r>, <sip:icscf2_p.home2.net/1r>,
<sip:token(<sip:scscf2.home2.net/1r>, <sip:icscf2_s.home2.net/1r>.)@home2.net;tokenized-
by=home2.net>, <sip:icscf1_s.home1.net/1r>, <sip:token(<sip:scscf1.home1.net/1r>,
<sip:icscf1_s.home1.net/1r>.)@home1.net;tokenized-by=home1.net>,
<sip:pcscf1.visited1.net/1r>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

27. 183 Session Progress (I-CSCF1b to S-CSCF1) - see example in table 17.5.2-27

I-CSCF1b forwards the 183 Session Progress response to the S-CSCF1.

Table 17.5.2-27: 183 Session Progress (I-CSCF1b to S-CSCF1)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:icscf2_p.home2.net;lr>,
<sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>@home2.net;tokenized-
by=home2.net>, <sip:icscf1_s.home1.net;lr>, <sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

28. 183 Session Progress (S-CSCF1 to I-CSCF1a) - see example in table 17.5.2-28

S-CSCF1 forwards the 183 Session Progress response to I-CSCF1a.

Table 17.5.2-28: 183 Session Progress (S-CSCF1 to I-CSCF1a)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP icscfl_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

29. 183 Session Progress (I-CSCF1a to P-CSCF1) - see example in table 17.5.2-29

I-CSCF1a forwards the 183 Session Progress response to P-CSCF1.

Table 17.5.2-29: 183 Session Progress (I-CSCF1a to P-CSCF1)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:icscf2_p.home2.net;lr>,
    <sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>)>@home2.net;tokenized-
    by=home2.net>, <sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
    <sip:icscf1_s.home1.net;lr>)>@home1.net;tokenized-by=home1.net>,
    <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

30. Authorize QoS Resources

P-CSCF1 authorizes the resources necessary for this new media.

31. 183 Session Progress (P-CSCF1 to UE1) - see example in table 17.5.2-31

P-CSCF1 forwards the 183 Session Progress response to the originating endpoint.

Table 17.5.2-31: 183 Session Progress (P-CSCF1 to UE1)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:icscf2_p.home2.net;lr>,
    <sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_s.home2.net;lr>)>@home2.net;tokenized-
    by=home2.net>, <sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
    <sip:icscf1_s.home1.net;lr>)>@home1.net;tokenized-by=home1.net>,
    <sip:pcscf1.visited1.net;7531;lr;comp=sigcomp>
P-Media-Authorization:
    0020000100100101706466312e76697369746564312e6e6574000c02013942563330373400
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
RSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

P-Media-Authorization: A P-CSCF generated authorization token. This particular example shows a Policy-Element generated by "pdf1.visited1.net" with credentials "9BV3074".

Record-Route: The P-CSCF rewrites the Record-Route header to add the port number negotiated in the security agreement and the comp=sigcomp parameter to its own SIP URI.

32. PRACK (UE1 to P-CSCF1) - see example in table 17.5.2-32

The originator decides the final set of media streams for this media addition, and sends the Final SDP to P-CSCF1.

Table 17.5.2-32: PRACK (UE1 to P-CSCF1)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:token(<sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>)>@home1.net;tokenized-by=home1.net>,
<sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_s.home2.net;lr>)>)>@home2.net;tokenized-by=home2.net>,
<sip:icscf2_p.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 133 PRACK
Require: precondition, sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
RAck: 9022 132 INVITE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907166275_0_0
m=audio 3456 RTP/AVP 97
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
m=video 9544 RTP/AVP 31
b=AS:54.6
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:31 H261/90000

```

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

33. PRACK (P-CSCF1 to I-CSCF1a) - see example in table 17.5.2-33

The PRACK request is forwarded through this I-CSCF to the S-CSCF.

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Proxy-Require header is empty, it removes this header completely.

Table 17.5.2-33: PRACK (P-CSCF1 to I-CSCF1a)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:icscf1_p.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>)@home1.net;tokenized-by=home1.net>,
<sip:icscf2_s.home2.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_p.home2.net;lr>)@home2.net;tokenized-by=home2.net>,
<sip:pcscf2.visited2.net;lr>
P-Access-Network-Info:
From:
To:
Call-ID:
Cseq:
Require: precondition
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

34. PRACK (I-CSCF1a to S-CSCF1) - see example in table 17.5.2-34

The PRACK request is forwarded through this I-CSCF1a to the S-CSCF1.

Table 17.5.2-34: PRACK (I-CSCF1a to S-CSCF1)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
   <sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr>@home2.net;tokenized-
   by=home2.net)>, <sip:pcscf2.visited2.net;lr>
P-Access-Network-Info:
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

35. PRACK (S-CSCF1 to I-CSCF1b) - see example in table 17.5.2-35

S-CSCF1 forwards the PRACK request to I-CSCF1b.

Table 17.5.2-35: PRACK (S-CSCF1 to I-CSCF1b)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:icscf1_s.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
    <sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr> )@home2.net;tokenized-
    by=home2.net>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

36. PRACK (I-CSCF1b to I-CSCF2a) - see example in table 17.5.2-36

I-CSCF1b forwards the PRACK request to I-CSCF2a.

Table 17.5.2-36: PRACK (I-CSCF1b to I-CSCF2a)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:icscf2_s.home2.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_p.home2.net;lr>@home2.net;tokenized-by=home2.net>,
<sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

37. PRACK (I-CSCF2a to S-CSCF2) - see example in table 17.5.2-37

I-CSCF2a forwards the PRACK request to S-CSCF2.

Table 17.5.2-37: PRACK (I-CSCF2a to S-CSCF2)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
     pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

38. PRACK (S-CSCF2 to I-CSCF2b) - see example in table 17.5.2-38

S-CSCF2 forwards the PRACK request to I-CSCF2b.

Table 17.5.2-39: PRACK (I-CSCF2b to P-CSCF2)

```

PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 63
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Require:
RAck:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

40. PRACK (P-CSCF2 to UE2) - see example in table 17.5.2-40

P-CSCF2 and forwards the PRACK request to the UE2.

Table 17.5.2-40: PRACK (P-CSCF2 to UE2)

```
PRACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 62
From:
To:
Call-ID:
Cseq:
Require:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

41. 200 OK (UE2 to P-CSCF2) - see example in table 17.5.2-41

UE2 acknowledges the PRACK request with a 200 OK response.

Table 17.5.2-41: 200 OK (UE2 to P-CSCF2)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscaf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=907166275-0 0
m=audio 6544 RTP/AVP 97
b=AS:25.4 3
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
m=video 7544 RTP/AVP 31
b=AS:54.6
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=conf:qos remote sendrecv
a=rtptime:31 H261/90000

```

42. Resource Reservation

After determining the final set of media streams for this additional media, UE2 initiates the reservation procedures for the additional resources needed for this new media.

43. 200 OK (P-CSCF2 to I-CSCF2b) - see example in table 17.5.2-43

P-CSCF2 forwards the 200 OK response to I-CSCF2b.

Table 17.5.2-44: 200 OK (I-CSCF2b to S-CSCF2)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

45. 200 OK (S-CSCF2 to I-CSCF2a) - see example in table 17.5.2-45

S-CSCF2 forwards the 200 OK response to I-CSCF2a.

Table 17.5.2-45: 200 OK (S-CSCF2 to I-CSCF2a)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

46. 200 OK (I-CSCF2a to I-CSCF1b) - see example in table 17.5.2-46

I-CSCF2a forwards the 200 OK response to I-CSCF1b.

Table 17.5.2-46: 200 OK (I-CSCF2a to I-CSCF1b)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

47. 200 OK (I-CSCF1b to S-CSCF1) - see example in table 17.5.2-47

S-CSCF forwards the 200 OK response to S-CSCF1.

Table 17.5.2-47: 200 OK (I-CSCF1b to S-CSCF1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
     pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

48. 200 OK (S-CSCF1 to I-CSCF1a) - see example in table 17.5.2-48

S-CSCF1 forwards the 200 OK response to I-CSCF1a.

Table 17.5.2-48: 200 OK (S-CSCF1 to I-CSCF1a)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
     pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

49. 200 OK (I-CSCF1a to P-CSCF1) - see example in table 17.5.2-49

I-CSCF1 forwards the 200 OK response to P-CSCF1.

Table 17.5.2-49: 200 OK (I-CSCF1a to P-CSCF1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

50. 200 OK (P-CSCF1 to UE1) - see example in table 17.5.2-50

P-CSCF1 forwards the 200 OK response to the originator.

Table 17.5.2-50: 200 OK (P-CSCF1 to UE1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

51. Resource Reservation

After determining the final set of media streams for this additional media, UE1 initiates the reservation procedures for the additional resources needed for this new media.

52. UPDATE (UE1 to P-CSCF1) - see example in table 17.5.2-52

When the resource reservation is completed, UE sends the UPDATE request to the terminating endpoint, via the signalling path established by the INVITE request.

Table 17.5.2-52: UPDATE (UE1 to P-CSCF1)

```

UPDATE sip: [5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:token(<sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>@home1.net;tokenized-by=home1.net>,
<sip:icscf1_s.home1.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_s.home2.net;lr>@home2.net;tokenized-by=home2.net>,
<sip:icscf2_p.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfgklkj490333
Cseq: 134 UPDATE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg= hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
c=8642; port-s=7531
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=907166275-0 0
m=audio 3456 RTP/AVP 97
b=AS:25.4
a=curr:qos local sendrecv
a=curr:qos remote sendrecv
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-periodmaxframes=2
a=rtptime:96 telephone-event
a=maxptime:20
m=video 9544 RTP/AVP 31
b=AS:54.6
a=curr:qos local sendrecv
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtptime:31 H261/90000

```

Security-Verify: Contains the security agreement as represented by the received Security-Server header.

53. UPDATE (P-CSCF1 to I-CSCF1a) - see example in table 17.5.2-53

The P-CSCF removes the Security-Verify header and associated "sec-agree" option-tags prior to forwarding the request. As the Require and Proxy-Require headers are empty, it removes these headers completely.

The UPDATE request is forwarded through this P-CSCF1 to the I-CSCF1a.

Table 17.5.2-53: UPDATE (P-CSCF1 to I-CSCF1a)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcsf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:icscf1_p.home1.net;lr>, <sip:token(<sip:scscf1.home1.net;lr>,
<sip:icscf1_s.home1.net;lr>@home1.net;tokenized-by=home1.net>,
<sip:icscf2_s.home2.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_p.home2.net;lr>@home2.net;tokenized-by=home2.net>,
<sip:pcscf2.visited2.net;lr>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024";
ggsn=[5555::4b4:3c3:2d2:1e1]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-sig=no;
gcid=A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no; gcid=F312D5E3BC; flow-
id=({2,1},{2,2})"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

54. UPDATE (I-CSCF1a to S-CSCF1) - see example in table 17.5.2-54

The UPDATE request is forwarded through this I-CSCF1a to the S-CSCF1.

Table 17.5.2-54: UPDATE (I-CSCF1a to S-CSCF1)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf1.home1.net;lr>, <sip:icscf1_s.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
<sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr>)&tokenized-
by=home2.net>, <sip:pcscf2.visited2.net;lr>
P-Access-Network-Info:
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

55. UPDATE (S-CSCF1 to I-CSCF1b) - see example in table 17.5.2-55

S-CSCF1 forwards the UPDATE request to I-CSCF1b.

Table 17.5.2-55: UPDATE (S-CSCF1 to I-CSCF1b)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:icscf1_s.home1.net;lr>, <sip:icscf2_s.home2.net;lr>,
    <sip:token(<sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr>)>@home2.net;tokenized-
    by=home2.net>, <sip:pcscf2.visited2.net;lr>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
    term-ioi=home2.net
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

56. UPDATE (I-CSCF1b to I-CSCF2a) - see example in table 17.5.2-56

I-CSCF1b forwards the UPDATE request, to I-CSCF2a.

Table 17.5.2-56: UPDATE (I-CSCF1b to I-CSCF2a)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Route: <sip:icscf2_s.home2.net;lr>, <sip:token(<sip:scscf2.home2.net;lr>,
<sip:icscf2_p.home2.net;lr>)@home2.net;tokenized-by=home2.net>,
<sip:pcscf2.visited2.net;lr>
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

57. UPDATE (I-CSCF2a to S-CSCF2) - see example in table 17.5.2-57

I-CSCF2a forwards the UPDATE request to S-CSCF2.

Table 17.5.2-57: UPDATE (I-CSCF2a to S-CSCF2)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Route: <sip:scscf2.home2.net;lr>, <sip:icscf2_p.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
P-Charging-Vector:
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

58. UPDATE (S-CSCF2 to I-CSCF2b) - see example in table 17.5.2-58

S-CSCF2 forwards the UPDATE request to I-CSCF2b.

Table 17.5.2-58: UPDATE (S-CSCF2 to I-CSCF2b)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
    icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
    icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
    scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 64
Route: <sip:icscf2_p.home2.net;lr>, <sip:pcscf2.visited2.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

59. UPDATE (I-CSCF2b to P-CSCF2) - see example in table 17.5.2-59

I-CSCF2b forwards the UPDATE request to P-CSCF2.

Table 17.5.2-60: UPDATE (P-CSCF2 to UE2)

```

UPDATE sip:[5555::eee:fff:aaa:bbb]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 62
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

61. 200 OK (UE2 to P-CSCF2) - see example in table 17.5.2-61

UE2 acknowledges the UPDATE request with a 200 OK response.

Table 17.5.2-61: 200 OK (UE2 to P-CSCF2)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq: 134 UPDATE
Content-Type:
Content-Length: 0

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=

```

62. 200 OK (P-CSCF2 to I-CSCF2b) - see example in table 17.5.2-62

Table 17.5.2-62: 200 OK (P-CSCF2 to I-CSCF2b)

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_p.home2.net;branch=z9hG4bK556u87.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
icscf2_s.home2.net;branch=z9hG4bK871y12.1)@home2.net;tokenized-by=home2.net, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=

```

63. 200 OK (I-CSCF2b to S-CSCF2) - see example in table 17.5.2-63

Table 17.5.2-63: 200 OK (I-CSCF2b to S-CSCF2)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
     icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
     icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
     scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
     icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
     pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
     [5555:aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

64. **200 OK (S-CSCF2 to I-CSCF2a) - see example in table 17.5.2-64**

Table 17.5.2-64: 200 OK (S-CSCF2 to I-CSCF2a)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

65. 200 OK (I-CSCF2a to I-CSCF1b) - see example in table 17.5.2-65

Table 17.5.2-65: 200 OK (I-CSCF2a to I-CSCF1b)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_s.home1.net;branch=z9hG4bK312a32.1, SIP/2.0/UDP token(SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
icscf1_p.home1.net;branch=z9hG4bK351g45.1)@home1.net;tokenized-by=home1.net, SIP/2.0/UDP
pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

66. 200 OK (I-CSCF1b to S-CSCF1) - see example in table 17.5.2-66

Table 17.5.2-66: 200 OK (I-CSCF1b to S-CSCF1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
    icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

67. 200 OK (S-CSCF1 to I-CSCF1a) - see example in table 17.5.2-67

Table 17.5.2-67: 200 OK (S-CSCF1 to I-CSCF1a)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

68. **200 OK (I-CSCF1a to P-CSCF1)** - see example in table 17.5.2-68

Table 17.5.2-68: 200 OK (I-CSCF1a to P-CSCF1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

69. **200 OK (P-CSCF1 to UE1)** - see example in table 17.5.2-69

Table 17.5.2-69: 200 OK (P-CSCF1 to UE1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
a=
a=
a=
a=
```

Remainder of subclause not shown

CR-Form-v7.1

CHANGE REQUEST

24.229 CR 869 # rev 1 # Current version: 5.12.0

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the # symbols.

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Port 5060		
Source:	# Ericsson		
Work item code:	# IMS-CCR	Date:	# 12/04/2005
Category:	# F	Release:	# Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	F (correction)		Ph2 (GSM Phase 2)
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)
	B (addition of feature),		R97 (Release 1997)
	C (functional modification of feature)		R98 (Release 1998)
	D (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)
			Rel-7 (Release 7)

Reason for change:	# RFC 3261 recommends, but not mandate, the port 5060 to be used for initial SIP communication. It is proposed to clearly specify that the UE should use port 5060 in case no other initial port number is given and to clearly specify that the P-CSCF must listen to at least port 5060.
Summary of change:	# Clearly specify that the well known port 5060 (recommended by RFC 3261) is used in IMS as the default port in case no port information is available in the UE
Consequences if not approved:	# No default port is specified for IMS, leading to that SIP registration and consequently all SIP communication can fail.

Clauses affected:	# 4.2A, 5.1.1.2, 5.2.2				
Other specs Affected:	#				
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Y	N				
<input type="checkbox"/>	<input checked="" type="checkbox"/>				
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/>				
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/>				
Other comments:	#				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** First change *****

4.2A Transport mechanisms

This document makes no requirement on the transport protocol used to transfer signalling information over and above that specified in RFC 3261 [26] clause 18. However, the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] subclause 18.1.1, even if a mechanism exists of discovering a maximum transmission unit size longer than 1500 bytes.

[For initial REGISTER requests, the UE and the P-CSCF shall apply port handling according to subclause 5.1.1.2 and subclause 5.2.2.](#)

[The UE and the P-CSCF shall send and receive request and responses other than initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 \[19\].](#)

***** Second change *****

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

[The UE shall send only the initial REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261 \[26\].](#)

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

- a) the Authorization header, with the username field, set to the value of the private user identity;
- b) the From header set to the SIP URI that contains the public user identity to be registered;
- c) the To header set to the SIP URI that contains the public user identity to be registered;
- d) the Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;
- e) the Via header containing the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field.

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

- f) the Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

- g) a Request-URI set to the SIP URI of the domain name of the home network;
- h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];
- i) the Supported header containing the option tag "path"; and
- j) if a security association exists, a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- a) store the expiration time of the registration for the public user identities found in the To header value;
- b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;
- c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;
- d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;
- e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and
- f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

***** Third change *****

5.2.2 Registration

The P-CSCF shall be prepared to receive only the initial REGISTER requests on the SIP default port values as specified in RFC 3261 [26]. The P-CSCF shall also be prepared to receive the initial REGISTER requests on the port advertised to the UE during the P-CSCF discovery procedure.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

- 1) insert a Path header in the request including an entry containing:
 - the SIP URI identifying the P-CSCF;
 - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

- 2) insert a Require header containing the option tag "path";
- 3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];
- 4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";
- 5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;
- 6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:
 - a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
 - b) if the security association the REGISTER request was received on, is an already established one, then:
 - the P-CSCF shall remove the Security-Verify header if it is present, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
 - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
 - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and
 - c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;
- 7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;
- 3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and

RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

- 5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;
- 2) associate the Service-Route header list with the registered public user identity;
- 3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

- 5) store the values received in the P-Charging-Function-Addresses header;
- 6) if a set of temporary security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- 7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

- 1) reduce the SIP level lifetime of the old set of security associations towards the same UE to $64 * T1$ (if currently longer than $64 * T1$); and
- 2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 3: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 4: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than $64 * T1$ and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly established set of security associations for further messages towards the UE as appropriate (see NOTE 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

- 1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;

- 2) keep the newly established set of security associations created during this authentication;
- 3) delete, if existing, any other set of security associations towards this UE immediately; and,
- 4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) response for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

- 1) keep the newly established set of security associations created during this authentication;
- 2) delete, if existing, any other set of security associations towards this UE immediately; and,
- 3) use the kept newly established set of security associations for further messages sent towards the UE.

NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2-1.

Table 5.2.2-1: Handling of security associations at the P-CSCF

	Temporary set of security associations	Newly established set of security associations	Old set of security associations
SIP message received over newly established set of security associations that have not yet been taken into use	No action	Take into use	Reduce SIP level lifetime to $64 \cdot T1$, if lifetime is larger than $64 \cdot T1$
SIP message received over old set of security associations	No action	No action	No action
Old set of security associations currently in use will expire in $64 \cdot T1$	No action	Take into use	No action
Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request	Create Remove any previously existing temporary set of security associations	No action	No action
Sending 200 (OK) response for REGISTER request that concludes re-authentication	Change to a newly established set of security associations	Convert to and treat as old set of security associations (see next column)	Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received. Delete all other old sets of security associations immediately
Sending 200 (OK) response for REGISTER request that concludes initial authentication	Change to a newly established set of security associations and take into use immediately	Convert to old set of security associations, i.e. delete	Delete

CR-Form-v7.1

CHANGE REQUEST

24.229 CR 871 # rev 1 # Current version: 6.6.0

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the # symbols.

Proposed change affects: UICC apps# ME Radio Access Network Core Network

Title:	# Port 5060				
Source:	# Ericsson				
Work item code:	# IMS-CCR	Date:	# 15/03/2005		
Category:	# A	Release:	# Rel-6		
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:		
	F (correction)		Ph2 (GSM Phase 2)		
	A (corresponds to a correction in an earlier release)		R96 (Release 1996)		
	B (addition of feature),		R97 (Release 1997)		
	C (functional modification of feature)		R98 (Release 1998)		
	D (editorial modification)		R99 (Release 1999)		
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)		
			Rel-5 (Release 5)		
			Rel-6 (Release 6)		
			Rel-7 (Release 7)		

Reason for change:	# RFC 3261 recommends, but not mandate, the port 5060 to be used for initial SIP communication. It is proposed to clearly specify that the UE should use port 5060 in case no other initial port number is given and to clearly specify that the P-CSCF must listen to at least port 5060.
Summary of change:	# Clearly specify that the well known port 5060 (recommended by RFC 3261) is used in IMS as the default port in case no port information is available in the UE
Consequences if not approved:	# No default port is specified for IMS, leading to that SIP registration and consequently all SIP communication can fail.

Clauses affected:	# 5.1.1.2, 5.2.2								
Other specs affected:	<table style="display: inline-table; border-collapse: collapse;"> <tr> <td style="border: 1px solid black; padding: 2px; text-align: center;">Y</td> <td style="border: 1px solid black; padding: 2px; text-align: center;">N</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px; text-align: center;"># <input type="checkbox"/></td> <td style="border: 1px solid black; padding: 2px; text-align: center;"># <input checked="" type="checkbox"/></td> </tr> <tr> <td style="border: 1px solid black; padding: 2px; text-align: center;"># <input type="checkbox"/></td> <td style="border: 1px solid black; padding: 2px; text-align: center;"># <input checked="" type="checkbox"/></td> </tr> <tr> <td style="border: 1px solid black; padding: 2px; text-align: center;"># <input type="checkbox"/></td> <td style="border: 1px solid black; padding: 2px; text-align: center;"># <input checked="" type="checkbox"/></td> </tr> </table> Other core specifications # Test specifications # O&M Specifications #	Y	N	# <input type="checkbox"/>	# <input checked="" type="checkbox"/>	# <input type="checkbox"/>	# <input checked="" type="checkbox"/>	# <input type="checkbox"/>	# <input checked="" type="checkbox"/>
Y	N								
# <input type="checkbox"/>	# <input checked="" type="checkbox"/>								
# <input type="checkbox"/>	# <input checked="" type="checkbox"/>								
# <input type="checkbox"/>	# <input checked="" type="checkbox"/>								
Other comments:	#								

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** First change *****

4.2A Transport mechanisms

This document makes no requirement on the transport protocol used to transfer signalling information over and above that specified in RFC 3261 [26] clause 18. However, the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] subclause 18.1.1, even if a mechanism exists of discovering a maximum transmission unit size longer than 1500 bytes.

For initial REGISTER requests, the UE and the P-CSCF shall apply port handling according to subclause 5.1.1.2 and subclause 5.2.2.

The UE and the P-CSCF shall send and receive request and responses other than initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [19].

***** Second change *****

5.1.1.2 Initial registration

The UE can register a public user identity with its contact address at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

The UE shall send only the initial REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261 [26].

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

- a) an Authorization header, with the username field, set to the value of the private user identity;
- b) a From header set to the SIP URI that contains the public user identity to be registered;
- c) a To header set to the SIP URI that contains the public user identity to be registered;
- d) a Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;
- e) a Via header set to include the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

- f) an Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

- g) a Request-URI set to the SIP URI of the domain name of the home network;
- h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];
- i) the Supported header containing the option tag "path"; and
- j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- a) store the expiration time of the registration for the public user identities found in the To header value;
- b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;
- c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;
- d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;
- e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and
- f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

***** Third change *****

5.2.2 Registration

The P-CSCF shall be prepared to receive only the initial REGISTER requests on the SIP default port values as specified in RFC 3261 [26]. The P-CSCF shall also be prepared to receive the initial REGISTER requests on the port advertised to the UE during the P-CSCF discovery procedure.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

- 1) insert a Path header in the request including an entry containing:
 - the SIP URI identifying the P-CSCF;
 - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;
- 2) insert a Require header containing the option tag "path";
- 3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

- 4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";
- 5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. If the header is not present, then the P-CSCF shall return a suitable 4xx response;
- 6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:
 - a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header;
 - b) if the security association the REGISTER request was received on, is an already established one, then:
 - the P-CSCF shall remove the Security-Verify header if it is present;
 - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
 - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and
 - c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;
- 7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;
- 3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routing information in the requests originated by the UE. If this registration is a re-registration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;
- 2) associate the Service-Route header list with the registered public user identity;
- 3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

- 5) store the values received in the P-Charging-Function-Addresses header;
- 6) if a temporary set of security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- 7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

- 1) reduce the SIP level lifetime of the old set of security associations towards the same UE to $64 * T1$ (if currently longer than $64 * T1$); and
- 2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 3: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 4: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than $64 * T1$ and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly established set of security associations for further messages towards the UE as appropriate (see NOTE 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

- 1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;
- 2) keep the newly established set of security associations created during this authentication;
- 3) delete, if existing, any other set of security associations towards this UE immediately; and

- 4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) response for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

- 1) keep the newly established set of security associations created during this authentication;
- 2) delete, if existing, any other set of security associations towards this UE immediately; and
- 3) use the kept newly established set of security associations for further messages sent towards the UE.

NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2-1.

Table 5.2.2-1: Handling of security associations at the P-CSCF

	Temporary set of security associations	Newly established set of security associations	Old set of security associations
SIP message received over newly established set of security associations that have not yet been taken into use	No action	Take into use	Reduce SIP level lifetime to 64*T1, if lifetime is larger than 64*T1
SIP message received over old set of security associations	No action	No action	No action
Old set of security associations currently in use will expire in 64*T1	No action	Take into use	No action
Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request	Create Remove any previously existing temporary set of security associations	No action	No action
Sending 200 (OK) response for REGISTER request that concludes re-authentication	Change to a newly established set of security associations	Convert to and treat as old set of security associations (see next column)	Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received. Delete all other old sets of security associations immediately
Sending 200 (OK) response for REGISTER request that concludes initial authentication	Change to a newly established set of security associations and take into use immediately	Convert to old set of security associations, i.e. delete	Delete

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 917** ⌘ rev **1** ⌘ Current version: **5.12.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Call-Id mismatch in the protected REGISTER when reg-await-auth timer is running		
Source:	⌘ Qualcomm Incorporated		
Work item code:	⌘ IMS-CCR	Date:	⌘ 28/4/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<p>Use <u>one</u> of the following categories:</p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>		<p>Use <u>one</u> of the following releases:</p> <p>Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)</p>

Reason for change:	⌘ Section 5.4.1.2.2 describes the normal execution path the S-CSCF takes when a protected REGISTER is received by the S-CSCF. It also specifies several conditions that must be fulfilled for the normal execution path to be taken. One of the conditions is that when the timer reg-await-auth is running and a protected REGISTER is received, the Call-Id in the received message must match the expected value.
	Section 5.4.1.2.3 describes the behavior of S-CSCF in abnormal conditions. However, this section does not describe the behavior of the S-CSCF when reg-await-auth timer is running and the received protected REGISTER contains a Call-Id different from the expected value.
Summary of change:	⌘ When reg-await-auth timer is running and the received protected REGISTER contains a Call-Id different from the expected value, the S-CSCF will send a 403-Forbidden response
Consequences if not approved:	⌘ Different implementations may send different responses, or silently discard the received message, leading to interoperability problems

Clauses affected:	⌘ 5.4.1.2.3						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<input checked="" type="checkbox"/>	Test specifications					
	<input checked="" type="checkbox"/>	O&M Specifications					

Other comments: ☹ This change is already made in R6 (N1-050076/NP-050073)

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☹ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.4 Procedures at the S-CSCF

5.4.1 Registration and authentication

[...]

5.4.1.2 Initial registration and user-initiated reregistration

[...]

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

- 1) check if the user needs to be reauthenticated.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

- 2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

- 1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.
- 2) stop timer reg-await-auth;
- 3) check whether an Authorization header is included, containing:
 - a) the private user identity of the user in the username field;
 - b) the algorithm which is AKAv1-MD5 in the algorithm field; and
 - c) the authentication challenge response needed for the authentication procedure in the response field.

The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

- 4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;
- 5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

- a) the list of public user identities associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,
- b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria;

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

- 6) bind to each non-barred registered public user identity all registered contact information and store the related method tag values from the Contact header for future use;

NOTE 2: There might be more than one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

- 7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- 8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

- 9) store the icid parameter received in the P-Charging-Vector header;

- 10) create a 200 (OK) response for the REGISTER request, including:

- a) the list of received Path headers;
- b) a P-Associated-URI header containing the list of public user identities that the user is authorized to use. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;
- c) a Service-Route header containing:
 - the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,
 - if network topology hiding is required a SIP URI identifying an I-CSCF (THIG) as the topmost entry; and
- d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;

- 11) send the so created 200 (OK) response to the UE;

- 12) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

- 13) handle the user as registered for the duration indicated in the Expires header.

5.4.1.2.3 Abnormal cases

In the case that the [REGISTER request that contains the](#) authentication challenge response [received](#) from the UE does not match with the expected [REGISTER request \(e.g. wrong Call-Id, wrong authentication challenge response\)](#) and the request has the "integrity-protected" parameter in the Authentication header set to "yes", the S-CSCF shall:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration time of the subscriber.

NOTE 1: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, which was supposed to carry the response to the challenge, contains no authentication challenge response and no AUTS parameters indicating that the MAC parameter was invalid in the challenge, the S-CSCF shall:

- respond with a 403 (Forbidden) response to the UE. The S-CSCF shall not update the registration time of the subscriber.

NOTE 2: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE containing an authentication challenge response indicates that the authentication challenge was invalid (contains the AUTS parameter indicating this), the S-CSCF will fetch new authentication vectors from the HSS. In order to indicate a resynchronisation, the S-CSCF shall include the AUTS received from the UE and the stored RAND when fetching the new authentication vectors. On receipt of the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or
- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned.

NOTE 3: Since the UE responds only to two consecutive challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the AS, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains more than one SIP URIs as Contact header entries, the S-CSCF shall only store the entry with the highest "q" value and include it in the 200 (OK) response.

NOTE 4: If the timer reg-await-auth expires, the S-CSCF will consider the authentication to have failed. If the public user identity was already registered, the S-CSCF will leave it as registered described in 3GPP TS 33.203 [19]. The operator's policy will specify when will, upon authentication failure, the currently registered public user identity or the user be de-registered by the S-CSCF.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 920** ⌘ rev **1** ⌘ Current version: **5.12.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Correction of error in the specification of the extension to Authorization header		
Source:	⌘ Qualcomm Incorporated		
Work item code:	⌘ IMS-CCR	Date:	⌘ 28/4/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ 'auth-param' is the ABNF non-terminal provided by RFC 2617 to permit applications to extend the headers defined in RFC 2617. 'auth-param' is used as a ABNF non-terminal in a number of header definitions in RFC 2617. Section 7.2A.2 defines a new parameter for Authorization Header. However, the non-terminal used in the ABNF ('integrity-protected') is a new non-terminal that is not used in RFC 2617. Hence it is unclear how this new definition would fit into the existing ABNF in RFC 2617.
Summary of change:	⌘ This CR changes the ABNF so that its relationship with the ABNF of Authorization Header given in RFC 2617 is clear. It also makes some text changes to make the supporting information precise, and the linkage with RFC 2617 precise and explicit.
Consequences if not approved:	⌘ Not clear how RFC 2617 is being enhanced by this specification. There would be no connection between the ABNF in RFC 2617 and the enhancements proposed in 24.229. Also there would be confusion between the auth-param defined in Section 7.2A.1 and Section 7.2A.2.

Clauses affected:	⌘ 7.2A.2						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						

Other comments: ☹

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☹ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7 Extensions within the present document

[...]

7.2A Extensions to SIP headers defined within the present document

[...]

7.2A.2 Extension to Authorization header

7.2A.2.1 Introduction

~~The integrity-protected authentication parameter~~ (This extension defines a new auth-param) ~~is an extension parameter defined~~ for the Authorization header used in REGISTER requests. For more information, see RFC 2617 [21] subclause 3.2.2.

7.2A.2.2 Syntax

The syntax ~~of for for~~ auth-param [for the Authorization header](#) is specified in table 7.5.

Table 7.5: Syntax of auth-param [for Authorization header](#)

```
integrity-protectedauth-param = "integrity-protected" EQUAL ("yes" / "no")
```

7.2A.2.3 Operation

This authentication parameter is inserted by the P-CSCF in [the Authorization header of](#) all the REGISTER requests received from the UE. The value of the "integrity protected" field in the auth-param parameter is set as specified in subclause 5.2.2. This information is used by S-CSCF to decide whether to challenge the REGISTER request or not, as specified in subclause 5.4.1.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 921** ⌘ rev **1** ⌘ Current version: **6.6.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Correction of error in the specification of the extension to Authorization header		
Source:	⌘ Qualcomm Incorporated		
Work item code:	⌘ IMS-CCR	Date:	⌘ 28/4/2005
Category:	⌘ A	Release:	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ 'auth-param' is the ABNF non-terminal provided by RFC 2617 to permit applications to extend the headers defined in RFC 2617. 'auth-param' is used as a ABNF non-terminal in a number of header definitions in RFC 2617. Section 7.2A.2 defines a new parameter for Authorization Header. However, the non-terminal used in the ABNF ('integrity-protected') is a new non-terminal that is not used in RFC 2617. Hence it is unclear how this new definition would fit into the existing ABNF in RFC 2617.
Summary of change:	⌘ This CR changes the ABNF so that its relationship with the ABNF of Authorization Header given in RFC 2617 is clear. It also makes some text changes to make the supporting information precise, and the linkage with RFC 2617 precise and explicit.
Consequences if not approved:	⌘ Not clear how RFC 2617 is being enhanced by this specification. There would be no connection between the ABNF in RFC 2617 and the enhancements proposed in 24.229. Also there would be confusion between the auth-param defined in Section 7.2A.1 and Section 7.2A.2. Lastly, possible inconsistency between Release 5 and Release 6 versions of this specification

Clauses affected:	⌘ 7.2A.2						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						

Other comments: ☹

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☹ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7 Extensions within the present document

[...]

7.2A Extensions to SIP headers defined within the present document

[...]

7.2A.2 Extension to Authorization header

7.2A.2.1 Introduction

~~The integrity-protected authentication parameter~~ [\(This extension defines a new auth-param\)](#) ~~is an extension parameter defined~~ for the Authorization header used in REGISTER requests. For more information, see RFC 2617 [21] subclause 3.2.2.

7.2A.2.2 Syntax

The syntax ~~of for for~~ auth-param [for the Authorization header](#) is specified in table 7.5.

Table 7.5: Syntax of auth-param [for Authorization header](#)

```
integrity-protectedauth-param = "integrity-protected" EQUAL ("yes" / "no")
```

7.2A.2.3 Operation

This authentication parameter is inserted by the P-CSCF in [the Authorization header of](#) all the REGISTER requests received from the UE. The value of the "integrity protected" field in the auth-param parameter is set as specified in subclause 5.2.2. This information is used by S-CSCF to decide whether to challenge the REGISTER request or not, as specified in subclause 5.4.1.

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 24.229 CR 922** ⌘ rev **-** ⌘ Current version: **5.12.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ SIP headers storage for P-CSCF initiated session release		
Source:	⌘ LM Ericsson		
Work item code:	⌘ IMS-CCR	Date:	⌘ 28/04/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ Information is missing in the current text		
Summary of change:	⌘ - Correction of SIP header values (To and From) to be stored for session initiation and target refresh requests/responses ⌘ - Addition of notes saying that new Contact header received in request is valid only if a reliable provisional response of 200 (OK) response is later received for the request ⌘ - Correction saying that Contact headers in target refresh responses are saved only for 1xx or 2xx responses ⌘ - Addition of text about SIP header values to be stored for non-target refresh requests within a dialog		
Consequences if not approved:	⌘ Implementations will not work in a desired way		

Clauses affected:	⌘ 5.2.6.3, 5.2.6.4, 5.2.8.1.2										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications Test specifications O&M Specifications	Y	N	⌘	X	⌘	X	⌘	X	⌘	
Y	N										
⌘	X										
⌘	X										
⌘	X										
Other comments:	⌘										

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ¶ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** FIRST MODIFICATION *****

5.2.6.3 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more than one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
 - b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;
- 2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:
 - a) the P-CSCF FQDN that resolves to the IP address, or
 - b) the P-CSCF IP address;
- 3) add its own SIP URI to the top of the Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:
 - a) the P-CSCF FQDN that resolves to the IP address; or
 - b) the P-CSCF IP address;
- 4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;
- 5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17]; and
- 6) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;
- 2) store the list of Record-Route headers from the received response;
- 3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;
- 4) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port values see 3GPP TS 33.203 [19].

- 5) if the response corresponds to an INVITE request, save the Contact, From, To and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
 - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;
 - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;
- 2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
 - b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog;
- 3) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:
 - a) the P-CSCF FQDN that resolves to the IP address, or
 - b) the P-CSCF IP address;
- 4) add its own SIP URI to the top of Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:
 - a) the P-CSCF FQDN that resolves to the IP address; or
 - b) the P-CSCF IP address; and

~~5) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;~~

5) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), replace the saved Contact and Cseq header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

NOTE: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the list of Record-Route headers from the received response;
- 2) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

- 3) ~~if the response corresponds to an INVITE request, save~~ replace the ~~saved~~ Contact ~~and Record-Route~~ header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for a standalone transaction, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
 - b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and
- 3) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
 - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;
 - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;
- 2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
 - b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog; and
- 3) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];

4) for INVITE dialogs, replace the saved Cseq header value received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
 - b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

***** SECOND MODIFICATION *****

5.2.6.4 Requests terminated by the UE

When the P-CSCF receives, destined for the UE, an initial request for a dialog, prior to forwarding the request, the P-CSCF shall:

- 1) remove its own SIP URI from the topmost Route header;
- 2) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;
- 3) if the request is an INVITE request, save a copy of the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;
- 4) add its own SIP URI to the top of the list of Record-Route headers and save the list. The P-CSCF SIP URI is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;
- 5) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 1: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 6) store the values received in the P-Charging-Function-Addresses header;

- 7) remove and store the icid parameter received in the P-Charging-Vector header; and
- 8) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request;
- 2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;
- 3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header list of this response. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Record-Route header values with those received in the request, rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter.

If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;
- 4) store the dialog ID and associate it with the private user identity and public user identity involved in the session; and
- 5) if the response corresponds to an INVITE request, save the Contact, [To](#), [From](#) and Record-Route header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

- 1) remove its own SIP URI from the topmost Route header value;
- 2) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

~~3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;~~

3) for INVITE dialogs, replace the saved Contact and Cseq header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

NOTE: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

When the P-CSCF receives ~~any~~ a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;
- 2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter; and
- 3) ~~if the response corresponds to an INVITE request, save~~ replace the saved Contact ~~and Record-Route~~ header field values ~~s~~ received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;
- 2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a request for a standalone transaction, or a request for an unknown method (that does not relate to an existing dialog), prior to forwarding the request, the P-CSCF shall:

- 1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 2) store the values received in the P-Charging-Function-Addresses header; and
- 3) remove and store the icid parameter received in the P-Charging-Vector header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request; and
- 2) remove the P-Preferred-Identity header, if present, and insert an P-Asserted-Identity header with the value saved from Request-URI of the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall:

- 1) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

NOTE 4: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 2) remove and store the icid parameter from P-Charging-Vector header;
- 3) [for INVITE dialogs, replace the saved Cseq header value received in the request such that the P-CSCF is able to release the session if needed;](#)

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

***** THIRD MODIFICATION *****

5.2.8.1.2 Release of an existing session

Upon receipt of an indication that the radio interface resources are no longer available for a served user, for whom one or more ongoing session exists, the P-CSCF shall release each of the related dialogs by applying the following steps:

- 1) if the P-CSCF serves the calling user of a session it shall generate a BYE request based on the information saved for the related dialog, including:
 - a Request-URI, set to the stored Contact header provided by the called user;
 - a To header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;

- a From header, set to the From header value as received in the initial INVITE request;
- a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
- a CSeq header, set to the current CSeq value ~~that was~~ stored for the direction from the calling to the called user, incremented by one;
- a Route header, set to the routing information towards the called user as stored for the dialog;
- further headers, based on local policy or the requested session release reason.

2) If the P-CSCF serves the called user of a session it shall generate a BYE request based on the information saved for the related dialog, including:

- a Request-URI, set to the stored Contact header provided by the calling user;
- a To header, set to the From header value as received in the initial INVITE request;
- a From header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
- a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
- a CSeq header, set to the current CSeq value ~~that was~~ stored for the direction from the called to the calling user, incremented by one—~~if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;~~
- a Route header, set to the routing information towards the calling user as stored for the dialog;
- further headers, based on local policy or the requested session release reason.

3) send the so generated BYE request towards the indicated user.

4) upon receipt of the 2xx responses for the BYE request, shall delete all information related to the dialog and the related multimedia session.

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 24.229 CR 891** ⌘ rev **2** ⌘ Current version: **6.6.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ SIP headers storage for P-CSCF initiated session release		
Source:	⌘ LM Ericsson		
Work item code:	⌘ IMS-CCR	Date:	⌘ 12/04/2005
Category:	⌘ A	Release:	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ Information is missing in the current text		
Summary of change:	⌘ - Correction of SIP header values (To and From) to be stored for session initiation and target refresh requests/responses ⌘ - Addition of notes saying that new Contact header received in request is valid only if a reliable provisional response of 200 (OK) response is later received for the request ⌘ - Correction saying that Contact headers in target refresh responses are saved only for 1xx or 2xx responses ⌘ - Addition of text about SIP header values to be stored for non-target refresh requests within a dialog		
Consequences if not approved:	⌘ Implementations will not work in a desired way		

Clauses affected:	⌘ 5.2.6.3, 5.2.6.4, 5.2.8.1.2						
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications	Y	N	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	Y	N	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						
	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	Y	N	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						
Other comments:	⌘						

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ¶ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** FIRST MODIFICATION *****

5.2.6.3 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more than one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
 - b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;
- 2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:
 - a) the P-CSCF FQDN that resolves to the IP address, or
 - b) the P-CSCF IP address;
- 3) add its own SIP URI to the top of the Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:
 - a) the P-CSCF FQDN that resolves to the IP address; or
 - b) the P-CSCF IP address;
- 4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;
- 5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and
- 6) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;
- 2) store the list of Record-Route headers from the received response;
- 3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;
- 4) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port values see 3GPP TS 33.203 [19].

- 5) if the response corresponds to an INVITE request, save the Contact, [From, To](#) and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
 - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;
 - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;
- 2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
 - b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog;
- 3) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:
 - a) the P-CSCF FQDN that resolves to the IP address, or
 - b) the P-CSCF IP address;
- 4) add its own SIP URI to the top of Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:
 - a) the P-CSCF FQDN that resolves to the IP address; or
 - b) the P-CSCF IP address; and

~~5) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;~~

5) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), replace the saved Contact and Cseq header filed values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

NOTE: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the list of Record-Route headers from the received response;
- 2) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

- 3) ~~if the response corresponds to an INVITE request, save~~ replace the ~~saved~~ Contact ~~and Record-Route~~ header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for a standalone transaction, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
 - b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and
- 3) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
 - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;
 - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;
- 2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
 - b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog; and
- 3) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

4) for INVITE dialogs, replace the saved Cseq header value received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
 - b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

******* SECOND MODIFICATION *******

5.2.6.4 Requests terminated by the UE

When the P-CSCF receives, destined for the UE, an initial request for a dialog, prior to forwarding the request, the P-CSCF shall:

- 1) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;
- 2) if the request is an INVITE request, save a copy of the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;
- 3) add its own SIP URI to the top of the list of Record-Route headers and save the list. The P-CSCF SIP URI is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;
- 4) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 1: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 5) store the values received in the P-Charging-Function-Addresses header;
- 6) remove and store the icid parameter received in the P-Charging-Vector header; and

- 7) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request;
- 2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;
- 3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header list of this response. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Record-Route header values with those received in the request, rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter.

If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;
- 4) store the dialog ID and associate it with the private user identity and public user identity involved in the session; and
- 5) if the response corresponds to an INVITE request, save the Contact, [To](#), [From](#) and Record-Route header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

- 1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

~~2) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;~~

2) for INVITE dialogs, replace the saved Contact and Cseq header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

NOTE: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

When the P-CSCF receives ~~any~~ a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;
- 2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter; and
- 3) ~~if the response corresponds to an INVITE request, save~~ replace the saved Contact ~~and Record-Route~~ header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

a) discard the response; or

b) replace the Via header values with those received in the request;

2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a request for a standalone transaction, or a request for an unknown method (that does not relate to an existing dialog), prior to forwarding the request, the P-CSCF shall:

- 1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 2) store the values received in the P-Charging-Function-Addresses header;
- 3) remove and store the icid parameter received in the P-Charging-Vector header; and
- 4) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request; and
- 2) remove the P-Preferred-Identity header, if present, and insert an P-Asserted-Identity header with the value saved from the P-Called-Party-ID header of the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall:

- 1) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:
 - a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

NOTE 4: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 2) remove and store the icid parameter from P-Charging-Vector header;
- 3) [for INVITE dialogs, replace the saved Cseq header value received in the request such that the P-CSCF is able to release the session if needed;](#)

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
 - a) discard the response; or
 - b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

***** THIRD MODIFICATION *****

5.2.8.1.2 Release of an existing session

Upon receipt of an indication that the radio interface resources are no longer available for a served user, for whom one or more ongoing session exists, the P-CSCF shall release each of the related dialogs by applying the following steps:

- 1) if the P-CSCF serves the calling user of a session it shall generate a BYE request based on the information saved for the related dialog, including:
 - a Request-URI, set to the stored Contact header provided by the called user;
 - a To header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;

- a From header, set to the From header value as received in the initial INVITE request;
 - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
 - a CSeq header, set to the current CSeq value ~~that was~~ stored for the direction from the calling to the called user, incremented by one;
 - a Route header, set to the routing information towards the called user as stored for the dialog;
 - further headers, based on local policy or the requested session release reason.
- 2) If the P-CSCF serves the called user of a session it shall generate a BYE request based on the information saved for the related dialog, including:
- a Request-URI, set to the stored Contact header provided by the calling user;
 - a To header, set to the From header value as received in the initial INVITE request;
 - a From header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
 - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
 - a CSeq header, set to the current CSeq value ~~that was~~ stored for the direction from the called to the calling user, incremented by one—~~if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;~~
 - a Route header, set to the routing information towards the calling user as stored for the dialog;
 - further headers, based on local policy or the requested session release reason.
- 3) send the so generated BYE request towards the indicated user.
- 4) upon receipt of the 2xx responses for the BYE request, shall delete all information related to the dialog and the related multimedia session.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 859** ⌘ rev **2** ⌘ Current version: **5.12.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ S-CSCF failure		
Source:	⌘ Lucent Technologies		
Work item code:	⌘ IMS-CCR	Date:	⌘ 15/04/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)

Reason for change:	⌘ The document 24.229-660 [Rel-6] subclause 5.3.1.3 specifies correctly that if the I-CSCF, upon receiving the REGISTER request that was integrity protected [i.e. it indicates that this is not an initial registration], will NOT forward the REGISTER request to the new S-CSCF. The I-CSCF will return an error response, i.e. the I-CSCF will indicate to the UE that the registration has failed. Subsequently, the UE SHOULD initiate a new initial registration and subscription to reg event to find out what are its valid registrations, and obtain a new Service-Route to the new S-CSCF. In addition, the UE may reregister the public user identities that were previously registered with the failed S-CSCF. <u>The document 24.229-5.12.0 [Rel-5] erroneously specifies that the I-CSCF will always select new S-CSCF.</u>
Summary of change:	⌘ Text added to correct the problem outlined above.
Consequences if not approved:	⌘ If the REGISTER request is forwarded to the new S-CSCF [and the UE receives the 200 OK], the UE would end up with being registered with two S-CSCFs - the failed S-CSCF and the new S-CSCF. Furthermore, the UE [upon receiving the 200 OK] would believe that all previous registrations are still valid.

Clauses affected:	⌘ 5.3.1.3 and 5.1.1.4						
Other specs	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						

affected:

<input checked="" type="checkbox"/>	Test specifications
<input checked="" type="checkbox"/>	O&M Specifications

Other comments: ☞

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>.

Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☞ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** CHANGE *******5.3.1.3 Abnormal cases**

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE. The response may include a Warning header containing the warn-code 399.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399.

If the the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 (Temporarily Unavailable) response to the UE.

If a selected S-CSCF:

- does not respond to the REGISTER request and its retransmissions by the I-CSCF; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response;

and:

- the REGISTER request did not include an "integrity-protected" parameter in the Authorization header; or
- did include an "integrity-protected" parameter with a value different from "yes" in the Authorization header;

the I-CSCF performs the user registration status query procedure with the HSS~~shall select a new S-CSCF~~ as described in subclause 5.3.1.2, and based on the capabilities indicated from the HSS, the I-CSCF shall select new S-CSCF. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If a selected S-CSCF does not respond to a REGISTER request and its retransmissions by the I-CSCF and the REGISTER request did include an Authorization header with the "integrity-protected" parameter set to "yes", the I-CSCF shall send back a 408 (Request Timeout) response or 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26].

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 (Busy Everywhere) response to the user.

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 24.229 CR 885** ⌘ rev **2** ⌘ Current version: **5.12.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Handling of P-Associated URI		
Source:	⌘ Ericsson		
Work item code:	⌘ IMS-CCR	Date:	⌘ 14/04/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<p>Use <u>one</u> of the following categories:</p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>		<p>Use <u>one</u> of the following releases:</p> <p>Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)</p>

Reason for change: ⌘ In section 5.1.1.2 it says that the UE shall store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity. Since there is no description of any manipulation of the list in the P-CSCF section or in a proxy section of RFC 3455 it implies that the information in the list sent from the S-CSCF is the same that is the same as received by the UE.

RFC 3455 also says that identities in the list is tied to address of record under registration, which is included in the TO header of the REGISTER request.

In addition, the P-CSCF shall associate the implicit registered public identity to the public user identity that was used to registration. This to make it possible for the P-CSCF to "remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities list and all related stored information", if it receives a 200 ok to a REGISTER when expire value is set to 0.

Summary of change: ⌘ It is clarified that P-CSCF shall tie the list received in the P-Associated URI to the Public User Identity under registration. The P-CSCF shall update the list of Public User Identities that the UE is allowed to use based on the information received in the Notify request .

The S-CSCF shall include in the list in the P-associated URI the non barred public user identities associated with the public user identity under registration.

Consequences if not approved: ⌘ It is unclear with the present wording what is included in the list in included in the P-Associated URI header, which willll lead to non compatible implementations.

Clauses affected: ⌘ 5.2.2, 5.2.4 5.2.5.2, 5.4.1.1.2.

	Y	N		⌘
Other specs Affected:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Test specifications	
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First change

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

- 1) insert a Path header in the request including an entry containing:
 - the SIP URI identifying the P-CSCF;
 - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;
- 2) insert a Require header containing the option tag "path";
- 3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];
- 4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";
- 5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;
- 6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:
 - a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
 - b) if the security association the REGISTER request was received on, is an already established one, then:
 - the P-CSCF shall remove the Security-Verify header if it is present, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
 - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
 - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and
 - c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;
- 7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;
- 3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;
- 2) associate the Service-Route header list with the registered public user identity;
- 3) ~~store the public user identities found in the P-Associated-URI header value, and associate them to the public user identity under registration as those that are authorized to be used by the UE;~~ and associate them to the public user identity under registration;
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

- 5) store the values received in the P-Charging-Function-Addresses header;
- 6) if a set of temporary security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- 7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

- 1) reduce the SIP level lifetime of the old set of security associations towards the same UE to $64 * T1$ (if currently longer than $64 * T1$); and
- 2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 3: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 4: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than $64 * T1$ and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly established set of security associations for further messages towards the UE as appropriate (see NOTE 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

- 1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;
- 2) keep the newly established set of security associations created during this authentication;
- 3) delete, if existing, any other set of security associations towards this UE immediately; and,
- 4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) response for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

- 1) keep the newly established set of security associations created during this authentication;
- 2) delete, if existing, any other set of security associations towards this UE immediately; and,
- 3) use the kept newly established set of security associations for further messages sent towards the UE.

NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2-1.

Table 5.2.2-1: Handling of security associations at the P-CSCF

	Temporary set of security associations	Newly established set of security associations	Old set of security associations
SIP message received over newly established set of security associations that have not yet been taken into use	No action	Take into use	Reduce SIP level lifetime to 64*T1, if lifetime is larger than 64*T1
SIP message received over old set of security associations	No action	No action	No action
Old set of security associations currently in use will expire in 64*T1	No action	Take into use	No action
Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request	Create Remove any previously existing temporary set of security associations	No action	No action
Sending 200 (OK) response for REGISTER request that concludes re-authentication	Change to a newly established set of security associations	Convert to and treat as old set of security associations (see next column)	Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received. Delete all other old sets of security associations immediately
Sending 200 (OK) response for REGISTER request that concludes initial authentication	Change to a newly established set of security associations and take into use immediately	Convert to old set of security associations, i.e. delete	Delete

Next change

5.2.4 Registration of multiple public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the P-CSCF shall maintain the generated dialog (identified by the values of the Call-ID, To and From headers).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package, the P-CSCF shall perform the following actions:

- if a state attribute "active", i.e. registered, is received for one or more public user identities, the P-CSCF shall
 - bind the indicated public user identities as registered to the contact information of the user; [and](#)
 - [add the public user identity to the list of the public user identities that are registered for the user.](#)
- if a state attribute "terminated", i.e. deregistered, is received for one or more public user identities, the P-CSCF shall release all stored information for these public user identities [and remove these public user identities from the list of the public user identities, that are registered for the user.](#)

NOTE: There may be public user identities which are implicitly registered within the registrar (S-CSCF) of the user upon registration of one public user identity. The procedures in this subclause provide a mechanism to inform the P-CSCF about these implicitly registered public user identities.

5.2.5.2 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.2.3, including one or more <registration> element(s) with the state attribute set to "terminated" the P-CSCF shall remove all stored information for these public user identities [and remove these public user identities from the list of the public user identities that are registered for the user.](#)

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header set to "terminated", the P-CSCF shall shorten the security associations towards the UE.

NOTE 1: The security association between the P-CSCF and the UE is shortened to a duration that will allow the NOTIFY request containing the deregistration event to reach the UE.

NOTE 2: When the P-CSCF receives the NOTIFY request with Subscription-State header containing the value of "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request to the S-CSCF with an Expires header containing a value of zero).

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

- 1) check if the user needs to be reauthenticated.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

- 2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

- 1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.
- 2) stop timer reg-await-auth;
- 3) check whether an Authorization header is included, containing:
 - a) the private user identity of the user in the username field;
 - b) the algorithm which is AKAv1-MD5 in the algorithm field; and
 - c) the authentication challenge response needed for the authentication procedure in the response field.

The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

- 4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;
- 5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

- a) the list of public user identities associated to the [public user identity under registration](#)-~~user~~, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,
- b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria;

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

- 6) bind to each non-barred registered public user identity all registered contact information and store the related method tag values from the Contact header for future use;

NOTE 2: There might be more than one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

- 7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- 8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

- 9) store the icid parameter received in the P-Charging-Vector header;

- 10) create a 200 (OK) response for the REGISTER request, including:

- a) the list of received Path headers;
- b) a P-Associated-URI header containing the list of public user identities that ~~the user is authorized to use~~ [are associated to the public user identity under registration](#). The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;

- c) a Service-Route header containing:

- the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,
- if network topology hiding is required a SIP URI identifying an I-CSCF(THIG) as the topmost entry; and

- d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;

- 11) send the so created 200 (OK) response to the UE;

- 12) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

- 13) handle the user as registered for the duration indicated in the Expires header.

CHANGE REQUEST

⌘ **TS 24.229** **CR 886** ⌘ rev **2** ⌘ Current version: **6.6.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Handling of P-Associated URI		
Source:	⌘ Ericsson		
Work item code:	⌘ IMS-CCR	Date:	⌘ 24/04/2005
Category:	⌘ A	Release:	⌘ Rel-6
	<p><i>Use <u>one</u> of the following categories:</i></p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>		<p><i>Use <u>one</u> of the following releases:</i></p> <p>Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)</p>

Reason for change:	⌘ In section 5.1.1.2 it says that the UE shall store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity. Since there is no description of any manipulation of the list in the P-CSCF section or in a proxy section of RFC 3455 it implies that the information in the list sent from the S-CSCF is the same that is the same as received by the UE.
	RFC 3455 also says that identities in the list is tied to address of record under registration, which is included in the TO header of the REGISTER request.
	In addition, the P-CSCF shall associate the implicit registered public identity to the public user identity that was used to registration. This to make it possible for the P-CSCF to "remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities and all related stored information", if it receives a 200 ok to a REGISTER when expire value is set to 0.
Summary of change:	⌘ It is clarified that P-CSCF shall tie the list received in the P-Associated URI to the Public User Identity under registration. The P-CSCF shall update the list of Public User Identities that the UE is allowed to use based on the information received in the Notify request.
	The S-CSCF shall include in the list in the P-associated URI the non barred public user identities associated with the public user identity under registration
Consequences if not approved:	⌘ It is unclear with the present wording what is included in the list in included in the P-Associated URI header, which will lead to non compatible implementations

Clauses affected:	⌘	5.2.2, 5.2.4, 5.2.5.2, and 5.4.1.2.2										
Other specs Affected:	⌘	<table border="1"><tr><td>Y</td><td>N</td></tr><tr><td></td><td>X</td></tr><tr><td></td><td>X</td></tr><tr><td></td><td>X</td></tr></table>	Y	N		X		X		X	Other core specifications	⌘
		Y	N									
			X									
	X											
	X											
	Test specifications											
	O&M Specifications											
Other comments:	⌘											

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First change

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

- 1) insert a Path header in the request including an entry containing:
 - the SIP URI identifying the P-CSCF;
 - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;
- 2) insert a Require header containing the option tag "path";
- 3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];
- 4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";
- 5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. If the header is not present, then the P-CSCF shall return a suitable 4xx response;
- 6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:
 - a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header;
 - b) if the security association the REGISTER request was received on, is an already established one, then:
 - the P-CSCF shall remove the Security-Verify header if it is present;
 - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
 - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and
 - c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;
- 7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;

- 2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;
- 3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 1: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;
- 2) associate the Service-Route header list with the registered public user identity;
- 3) store the public user identities found in the P-Associated-URI header value and associate them to the public user identity under registration. ~~as those that are authorized to be used by the UE;~~
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 2: There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

- 5) store the values received in the P-Charging-Function-Addresses header;
- 6) if a temporary set of security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- 7) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

- 1) reduce the SIP level lifetime of the old set of security associations towards the same UE to $64 * T1$ (if currently longer than $64 * T1$); and
- 2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 3: In this case, the P-CSCF will send requests towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 4: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than $64 * T1$ and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly established set of security associations for further messages towards the UE as appropriate (see NOTE 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

- 1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;
- 2) keep the newly established set of security associations created during this authentication;
- 3) delete, if existing, any other set of security associations towards this UE immediately; and
- 4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) response for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

- 1) keep the newly established set of security associations created during this authentication;
- 2) delete, if existing, any other set of security associations towards this UE immediately; and
- 3) use the kept newly established set of security associations for further messages sent towards the UE.

NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2-1.

Next change

5.2.4 Registration of multiple public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the P-CSCF shall maintain the generated dialog (identified by the values of the Call-ID, To and From headers).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package of the user, the P-CSCF shall perform the following actions:

- 1) for each public user identity whose state attribute in the <registration> element is set to "active", i.e. registered; and
 - the state attribute within the <contact> sub-element is set to "active"; and
 - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and
 - the event attribute of that <contact> sub-element(s) is set to "registered" or "created";

the P-CSCF shall

- bind the indicated public user identity as registered to the contact information of the respective user; [and](#)
- add the public user identity to the list of the public user identities that are registered for the user;

2) for each public user identity whose state attribute in the <registration> element is set to "active", i.e. registered: and

- the state attribute within the <contact> sub-element is set to "terminated";
- the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and
- the event attribute of that <contact> sub-element(s) is set to "deactivated", "expired", "probation", "unregistered", or "rejected";

the P-CSCF shall consider the indicated public user identity as deregistered for this user, and shall release all stored information for the public user identity bound to the respective user; and

3) for each public user identity whose state attribute in the <registration> element is set to "terminated", i.e. deregistered; and

- the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and
- the event attribute of that <contact> sub-element(s) is set to "deactivated", "expired", "probation", "unregistered", or "rejected";

the P-CSCF shall consider the indicated public user identity as deregistered for this UE, and shall release all stored information for these public user identity bound to the respective user [and remove the public user identity from the list of the public user identities that are registered for the user.](#)

If all public user identities, that were registered by the user using its private user identity, have been deregistered, the P-CSCF may either unsubscribe to the reg event package of the user or let the subscription expire.

NOTE: There may be public user identities which are implicitly registered within the registrar (S-CSCF) of the user upon registration of one public user identity. The procedures in this subclause provide a mechanism to inform the P-CSCF about these implicitly registered public user identities.

Next change

5.2.5.2 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package of the UE, as described in subclause 5.2.3, including one or more <registration> element(s) which were registered by the UE with either:

- the state attribute set to "terminated"; or
- the state attribute set to "active" and the state attribute within the <contact> sub-element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

the P-CSCF shall remove all stored information for these public user identities for this UE [and remove these public user identities from the list of the public user identities that are registered for the user.](#)

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header set to "terminated" or when all public user identities of the UE have been deregistered, the P-CSCF shall shorten the security associations towards the UE.

NOTE 1: The security association between the P-CSCF and the UE is shortened to a value that will allow the NOTIFY request containing the deregistration event to reach the UE.

NOTE 2: When the P-CSCF receives the NOTIFY request with Subscription-State header containing the value of "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request to the S-CSCF with an Expires header containing a value of zero).

Next change

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

- 1) check if the user needs to be reauthenticated.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

- 2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

- 1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.
- 2) stop timer reg-await-auth;
- 3) check whether an Authorization header is included, containing:
 - a) the private user identity of the user in the username field;
 - b) the algorithm which is AKAv1-MD5 in the algorithm field; and
 - c) the authentication challenge response needed for the authentication procedure in the response field.

The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

- 4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;
- 5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], store the following information in the local data:

- a) the list of public user identities associated to the ~~user~~ [the public user identity under registration](#), including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,
- b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria (the initial Filter Criteria for the Registered and common parts is stored and the unregistered part is retained for possible use later - in the case of the S-CSCF is retained if the user becomes unregistered);

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

- 6) bind to each non-barred registered public user identity all registered contact information including all header parameters contained in the Contact header and all associated URI parameters and store information for future use;

NOTE 2: There might be more than one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

- 7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- 8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;
- 9) store the icid parameter received in the P-Charging-Vector header;
- 10) create a 200 (OK) response for the REGISTER request, including:

- a) the list of received Path headers;
- b) a P-Associated-URI header containing the list of public user identities that ~~the user is authorized to use~~ [are associated to the public user identity under registration](#). The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;
- c) a Service-Route header containing:
 - the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,
 - if network topology hiding is required a SIP URI identifying an I-CSCF (THIG) as the topmost entry;
- d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request; and
- e) a Contact header listing all contact addresses for this public user identity.

NOTE 5: There might be other contact addresses available, that other UEs have registered for the same public user identity.

- 11) send the so created 200 (OK) response to the UE;

12) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 6: If this registration is a reregistration, the Filter Criteria already exists in the local data.

13) handle the user as registered for the duration indicated in the Expires header.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 906** ⌘ rev **2** ⌘ Current version: **5.c.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Clarification to the procedures at the I-CSCF		
Source:	⌘ Huawei		
Work item code:	⌘ IMS-CCR	Date:	⌘ 13/04/2005
Category:	⌘ F	Release:	⌘ Rel-5
	<p><i>Use <u>one</u> of the following categories:</i></p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>		<p><i>Use <u>one</u> of the following releases:</i></p> <p>Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)</p>

Reason for change:	⌘ For the registration procedure at the I-CSCF, it describes the handling of the I-CSCF if the user registration status query response from the HSS includes a valid SIP URI or a list of capabilities. However it does not mention the handling at the I-CSCF if the user registration status query response from the HSS includes both a valid SIP URI and a list of capabilities. According to the IMS stage 2 specification TS 23.228, it is possible that the HSS returns both a valid SIP URI and a list of capabilities, so the related description should be added in the IMS stage 3 specification.
Summary of change:	⌘ Add the description about the handling of the I-CSCF if the user registration status query response from the HSS includes both a valid SIP URI and a list of capabilities.
Consequences if not approved:	⌘ If the HSS returns both a SIP URI and a list of capabilities in the user registration status query response, the handling at the I-CSCF is missing.

Clauses affected:	⌘ 5.3.1.2										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	⌘	X	⌘	X	⌘	X	Other core specifications Test specifications O&M Specifications	⌘
Y	N										
⌘	X										
⌘	X										
⌘	X										
Other comments:	⌘										

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>.

Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.3.1 Registration procedure

5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

- 1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;
- 2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

- 1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more than one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;
- 2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the REGISTER request to the selected S-CSCF.

If the user registration status query response from the HSS includes both a list of capabilities and a valid SIP URI, the I-CSCF shall first use the SIP URI to select the S-CSCF, and then if the S-CSCF is not reachable, the I-CSCF shall select a new S-CSCF as indicated in the abnormal cases of subclause 5.3.1.3.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 907** ⌘ rev **2** ⌘ Current version: **6.6.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Clarification to the procedures at the I-CSCF		
Source:	⌘ Huawei		
Work item code:	⌘ IMS-CCR	Date:	⌘ 13/04/2005
Category:	⌘ A	Release:	⌘ Rel-6
	<p><i>Use <u>one</u> of the following categories:</i></p> <p>F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p>		<p><i>Use <u>one</u> of the following releases:</i></p> <p>Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7)</p>

Reason for change:	⌘ For the registration procedure at the I-CSCF, it describes the handling of the I-CSCF if the user registration status query response from the HSS includes a valid SIP URI or a list of capabilities. However it does not mention the handling at the I-CSCF if the user registration status query response from the HSS includes both a valid SIP URI and a list of capabilities. According to the IMS stage 2 specification TS 23.228, it is possible that the HSS returns both a valid SIP URI and a list of capabilities, so the related description should be added in the IMS stage 3 specification.
Summary of change:	⌘ Add the description about the handling of the I-CSCF if the user registration status query response from the HSS includes both a valid SIP URI and a list of capabilities.
Consequences if not approved:	⌘ If the HSS returns both a SIP URI and a list of capabilities in the user registration status query response, the handling at the I-CSCF is missing.

Clauses affected:	⌘ 5.3.1.2										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> </table>	Y	N		X		X		X	Other core specifications Test specifications O&M Specifications	⌘
Y	N										
	X										
	X										
	X										
Other comments:	⌘										

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>.

Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.3 Procedures at the I-CSCF

5.3.1 Registration procedure

5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

NOTE: Different UEs, each with its own private user identity, may register the same public user identity. Registrations for the same shared public user identity are directed to the same S-CSCF as described in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

- 1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;
- 2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

- 1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more than one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;
- 2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the REGISTER request to the selected S-CSCF.

If the user registration status query response from the HSS includes both a list of capabilities and a valid SIP URI, the I-CSCF shall first use the SIP URI to select the S-CSCF, and then if the S-CSCF is not reachable, the I-CSCF shall select a new S-CSCF as indicated in the abnormal cases of subclause 5.3.1.3.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.