3GPP TSG-CN Meeting #23 **NP-040026**
10th - 12th March 2004. Phoenix, USA.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards 24.228**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **2** CRs, **Rel-5** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1 in CN1#33 meeting**, and are forwarded to TSG CN Plenary meeting #23 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level	Meeting-2nd-Level
24.228	127	1	Rel-5	P-Charging-Function-Addresses header	F	5.7.0	5.8.0	N1-040495	N1-33
24.228	128		Rel-5	Editorial modification in notation conventions	F	5.7.0	5.8.0	N1-040335	N1-33

3GPP TSG-CN1 Meeting #33 **Tdoc N1-040495~~288~~**
Atlanta, Georgia, USA 16 – 20 February 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.228** **CR** **127** ⌘**rev** **1** ⌘ Current version: **5.7.0** ⌘

*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:	⌘	P-Charging-Function-Addresses header
Source:	⌘	Orange
Work item code:	⌘	IMS-CCR
Date:	⌘	21/01/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
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.

Use one of the following releases:

2	*(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)*

Reason for change:	⌘	Missing information on P-Charging-Function-Addresses header
Summary of change:	⌘	In TS 32.225 (§ 5.1.2.1.2+ § 5.1.1), it is required that the P-CSCF and I-CSCF can send Accounting requests towards the CCF based on REGISTER event after reception of 200 OK. For that purpose, the I-CSCF and P-CSCF need the CCF address. This CR adds the fact that S-CSCF inserts P-Chrging-Function-Addresses header in the 200 OK message in response to REGISTER. When P-CSCF is in a visited network compared to S-CSCF, then I-CSCF has to remove this header.
Consequences if not approved:	⌘	Inconsitent specification and misalignement with stage 2

Clauses affected:	⌘	6.2, 6.3, 16.2, 16.3

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	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.

XXXXXXXXXXXXXXXXXXXXXX FIRST CHANGES XXXXXXXXXXXXXXXXXXXXX

6.2 Registration signalling: user not registered

Figure 6.2-1 shows the registration signalling flow for the scenario when the user is not registered. For the purpose of this registration signalling flow, the subscriber is considered to be roaming. This flow also shows the authentication of the private user identity. In this signalling flow, the home network does not have network configuration hiding active.

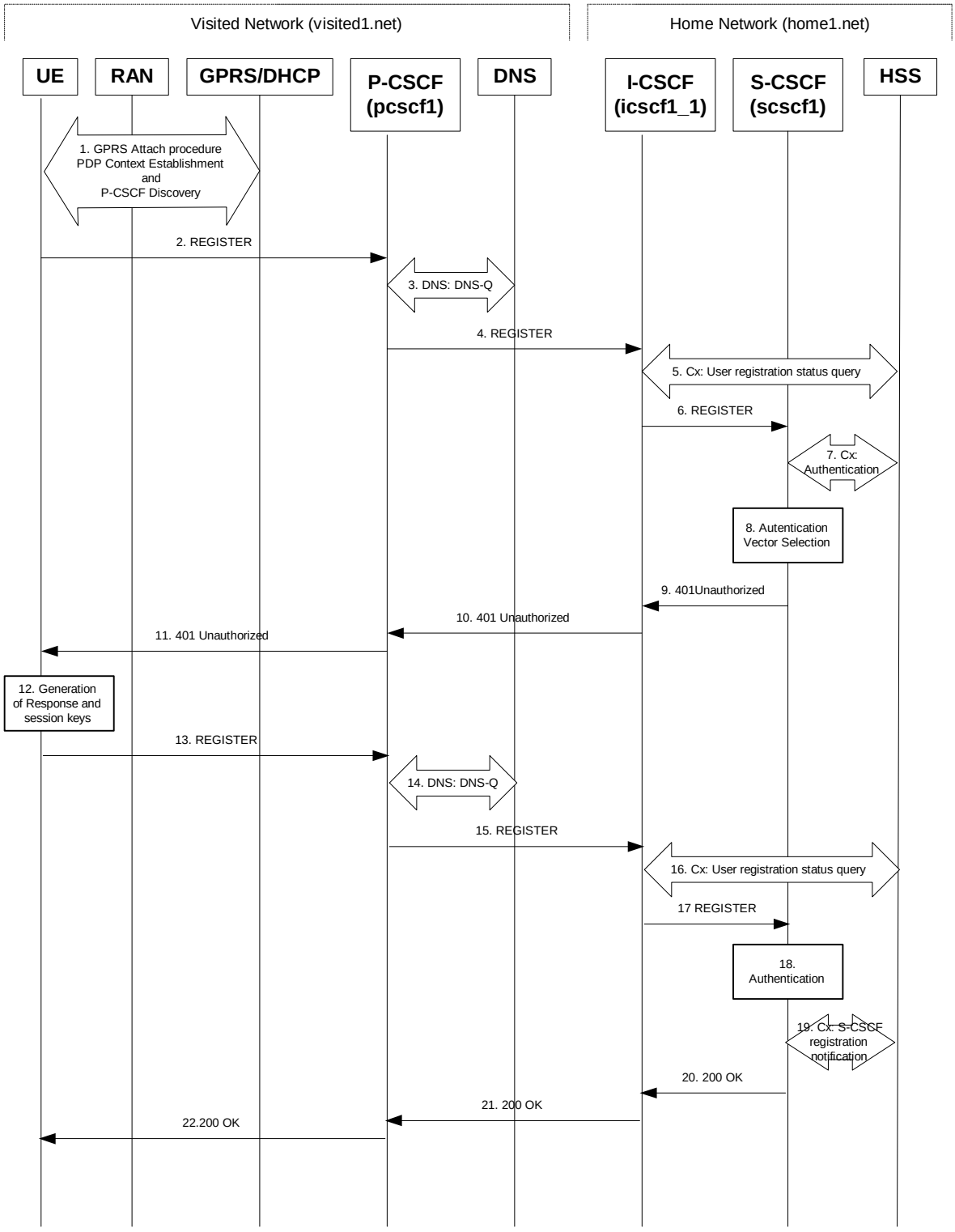

Figure 6.2-1: Registration signalling: user not registered

1. **GPRS Attach / PDP Context Establishment and P-CSCF Discovery (UE to GPRS)**

   This signalling flow is shown to indicate prerequisites for the registration signalling.

   See subclause 5.2 for details.

2. **REGISTER request (UE to P-CSCF) – see example in table 6.2-2**

   The purpose of this request is to register the user's SIP URI with a S-CSCF in the home network. This request is routed to the P-CSCF because it is the only SIP server known to the UE.

Table 6.2-2: REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd];comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce="", uri="sip:registrar.home1.net", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-c=2468;
   port-s=1357
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 1 REGISTER
Supported: path
Content-Length: 0
```

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("registrar.home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Via: IPv6 address of the UE allocated during the PDP Context Activation process.

Max-Forwards: Set to 70 by the UE and used to prevent loops.

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

From: This indicates the public user identity originating the REGISTER request. The public user identity may be obtained from the USIM.

To: This indicates the public user identity being registered. This is the identity by which other parties know this subscriber. It may be obtained from the USIM.

Contact: This indicates the point-of-presence for the subscriber - the IP address of the UE. This is the temporary point of contact for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the S-CSCF.

Authorization: It carries authentication information. The private user identity (user1_private@home1.net) is carried in theusername field of the Digest AKA protocol. The uri parameter (directive) contains the same value as the Request-URI. The realm parameter (directive) contains the network name where the username is authenticated. The Request-URI and the realm parameter (directive) value are obtained from the same field in the USIM and therefore, are identical. In this example, it is assumed that a new UICC card was just inserted into the terminal, and there is no other cached information to send. Therefore, nonce and response parameters (directives) are empty.

Security-Client: Lists the supported algorithm(s) by the UE.

Supported: This header is included to indicate to the recipient that the UE supports the Path header.

Upon receiving this request the P-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

3. **DNS: DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs the DNS queries to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI.

The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify a numeric IP address, and the transport protocol and port number are not indicated, the P-CSCF performs an NAPTR query for the domain specified in the Request-URI.

Table 6.2-3a DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=registrar.home1.net, QCLASS=IN, QTYPE=NAPTR
```

The DNS records are retrieved according to RFC 3263 [14].

Table 6.2-3b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=registrar.home1.net,  QCLASS=IN, QTYPE=NAPTR

registrar.home1.net          0 IN NAPTR 50   50 "s" "SIP+D2U"    ""
     _sip._udp.registrar.home1.net
                    0 IN NAPTR 90   50 "s" "SIP+D2T"    ""  _sip._tcp.registrar.home1.net
                          0 IN NAPTR 100  50 "s" "SIPS+D2T"   ""
     _sips._tcp.registrar.home1.net
```

Based on the order and preference of the NAPTR record and the local preference, UDP is preferred and the P-CSCF finds the I-CSCF by a DNS SRV lookup according to RFC 2782 [4].

Table 6.2-3c: DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=_sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

The DNS records are retrieved according to RFC 2782 [4].

Table 6.2-3d: DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=_sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net        0 IN SRV 1 10 5060 icscf1_p.home1.net
                                     0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

4. **REGISTER request (P-CSCF to I-CSCF) - see example in table 6.2-4**

The P-CSCF needs to be in the path for all mobile terminated requests for this user. To ensure this, the P-CSCF adds itself to the Path header value for future requests.

The P-CSCF binds the public user identity under registration to the Contact header supplied by the user.

The P-CSCF adds also the P-Visited-Network-ID header with the contents of the identifier of the P-CSCF network. This may be the visited network domain name or any other identifier that identifies the visited network at the home network.

This signalling flow shows the REGISTER request being forward from the P-CSCF to the I-CSCF in the home domain.

The P-CSCF removes the Security-Client 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 6.2-4: REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.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];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce="", uri="sip:registrar.home1.net", response="", integrity-protected="no"
CSeq:
Supported:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating requests.

Require: This header is included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

P-Visited-Network-ID: It contains the identifier of the P-CSCF network at the home network.

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

5. **Cx: User registration status query procedure**

The I-CSCF makes a request for information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

For detailed message flows see 3GPP TS 29.228.

Table 6.2-5a provides the parameters in the REGISTER request (flow 4) which are sent to the HSS.

Table 6.2-5a Cx: User registration status query procedure (I-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
I-CSCF to HSS	Private User Identity	Authorization:	The Private User Identity is encoded in the username field according to the Authorization protocol.
	Public User Identity	To:	Identity which is used to communicate with other users
	Visited Network Identifier	P-Visited-Network-ID:	This information indicates the network identifier of the visited network

6. **REGISTER request (I-CSCF to S-CSCF) – see example in table 6.2-6**

I-CSCF does not modify the Path header.

This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected.

Table 6.2-6: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.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];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info:
Path:
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Supported:
Content-Length:
```

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

Path: The S-CSCF stores the contents of the Path header and uses the URI for routing mobile terminated requests.

Upon receiving this request the S-CSCF may set its SIP registration timer for this UE to the Expires time in this request or the S-CSCF may assign another registration timer for this registration

7. **Cx: Authentication procedure**

As the REGISTER request arrived without integrity protection to the P-CSCF, the S-CSCF shall challenge it. For this, the S-CSCF requires at least one authentication vector to be used in the challenge to the user. If a valid AV is not available, then the S-CSCF requests at least one AV from the HSS.

The S-CSCF indicates to the HSS that it has been assigned to serve this user.

For detailed message flows see 3GPP TS 29.228.

Table 6.2-7a provides the parameters in the REGISTER request (flow 6) which are sent to the HSS.

Table 6.2-7a Cx: S-CSCF authentication information procedure (S-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
S-CSCF to HSS	Public User Identify	To:	Identity which is used to communicate with other users
	Private User Identity	Authorization:	The Private User Identity is encoded in the username field according to the Authorization protocol.
	S-CSCF Name	Request-URI:	This information element contains the name of the S-CSCF. The presence of this IE indicates that the user has not been authenticated yet by the S-CSCF

8. **Authentication vector selection**

The S-CSCF selects an authentication vector for use in the authentication challenge. For detailed description of the authentication vector, see 3GPP TS 33.203.

NOTE 1: The authentication vector may be of the form as in 3GPP TS 33.203 (if IMS AKA is the selected authentication scheme):

- $AV = RAND_n||AUTN_n||XRES_n||CK_n||IK_n$ where:
  - RAND: random number used to generate the XRES, CK, IK, and part of the AUTN. It is also used to generate the RES at the UE.
  - AUTN: Authentication token (including MAC and SQN).
  - XRES: Expected (correct) result from the UE.
  - CK: Cipher key (optional).
  - IK: Integrity key.

9. **401 Unauthorized response (S-CSCF to I-CSCF) - see example in table 6.2-9**

The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 6.2-9: 401 Unauthorized response (S-CSCF to I-CSCF)

```
SIP/2.0 401 Unauthorized
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];comp=sigcomp;branch=z9hG4bKnashds7
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Call-ID: apb03a0s09dkjdfglkj49111
WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN + server
   specific data), algorithm=AKAv1-MD5, ik="00112233445566778899aabbccddeeff",
   ck="ffeeddccbbaa11223344556677889900"
CSeq: 1 REGISTER
Content-Length: 0
```

WWW-Authenticate: The S-CSCF challenges the user. The nonce includes the quoted string, base64 encoded value of the concatenation of the AKA RAND, AKA AUTN and server specific data. The S-CSCF appends also the Integrity Key (IK) and the Cyphering key (CK).

NOTE 2: The actual nonce value in the WWW-Authenticate header field is encoded in base64, and it may look like: nonce="A34Cm+Fva37UYWpGNB34JP"

10. **401 Unauthorized response (I-CSCF to P-CSCF) - see example in table 6.2-10**

The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 6.2-10: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
WWW-Authenticate:
CSeq:
Content-Length:
```

11. **401 Unauthorized response (P-CSCF to UE) - see example in table 6.2-11**

The P-CSCF removes any keys received in the 401 Unauthorized response and forwards the rest of the response to the UE.

Table 6.2-11: 401 Unauthorized response (P-CSCF to UE)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN + server
   specific data), algorithm=AKAv1-MD5
Security-Server: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
   c=8642; port-s=7531
CSeq:
Content-Length:
```

WWW-Authenticate: The P-CSCF removes the ik and ck parameters (directives) from the header.

Security-Server: q is the preference value, 0.1 means IPsec is the first preferred choice. The q value represents only relative degradation of all mechanisms listed here. The lower value, the higher prority.

12. **Generation of response and session keys at UE**

Upon receiving the Unauthorised response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the authentication challenge response (using RES and other parameters as defined in RFC 3310 [18]), and also computes the session keys IK and CK. The authentication challenge response is put into the Authorization header and sent back to the registrar in the REGISTER request.

13. **REGISTER request (UE to P-CSCF) - see example in table 6.2-13**

Table 6.2-13 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.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
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
   uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1"
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-c=2468;
   port-s=1357
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
   c=8642; port-s=7531
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 2 REGISTER
Supported: path
Content-Length: 0
```

Authorization: This carries the response to the authentication challenge received in step 11 along with the private user identity, the realm, the nonce, the URI and the algorithm.

This message is protected by the IPsec SA negotiated.

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

14. **DNS: DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs the DNS queries to locate the I-CSCF in the home network. The look up in the DNS is based on the domain name specified in the Request URI.

The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify a numeric IP address, and the transport protocol and port number are not indicated, the P-CSCF performs an NAPTR query for the domain specified in the Request-URI.

Table 6.2-14a DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=registrar.home1.net, QCLASS=IN, QTYPE=NAPTR
```

The DNS records are retrieved according to RFC 3263 [14].

Table 6.2-14b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=registrar.home1.net,  QCLASS=IN, QTYPE=NAPTR

registrar.home1.net          0 IN NAPTR 50   50 "s" "SIP+D2U"    ""
     _sip._udp.registrar.home1.net
                    0 IN NAPTR 90   50 "s" "SIP+D2T"    ""  _sip._tcp.registrar.home1.net
                    0 IN NAPTR 100  50 "s" "SIPS+D2T"   ""  _sips._tcp.registrar.home1.net
```

Based on the order and preference of the NAPTR record and the local preference, UDP is preferred and the P-CSCF finds the I-CSCF by an DNS SRV lookup according to RFC 2782 [4].

Table 6.2-14c DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

The DNS records are retrieved according to RFC 2782 [4].

Table 6.2-14d DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net        0 IN SRV 1 10 5060 icscf1_p.home1.net
                                     0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

15. **REGISTER request (P-CSCF to I-CSCF) - see example in table 6.2-15**

This signalling flow shows the REGISTER request being forwarded from the P-CSCF to the I-CSCF in the home domain.

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 6.2-15 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.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
P-Access-Network-Info:
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
   uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-
   protected="yes"
CSeq:
Supported:
Content-Length:
```

Path: This is the P-CSCF URI and it is included to inform the S-CSCF where to route terminating requests.

16. **Cx: User registration status query procedure**

The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF name which was previously selected in step 5 (Cx: User registration status query procedure).

For detailed message flows see 3GPP TS 29.228.

Table 6.2-16a provides the parameters in the REGISTER request (flow 15), which are sent to the HSS.

Table 6.2-16a Cx: User registration status query procedure (I-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
I-CSCF to HSS	Private User Identity	Authorization:	The Private User Identity is encoded in the username field according to the Authorization protocol.
	Public User Identity	To:	Identity which is used to communicate with other users
	Visited Network Identifier	P-Visited-Network-ID:	This information indicates the network identifier of the visited network

17. **REGISTER request (I-CSCF to S-CSCF) - see example in table 6.2-17**

This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF.

Table 6.2-17: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.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
P-Access-Network-Info:
Path:
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Supported:
Content-Length:
```

Path: The S-CSCF stores the contents of the Path header and uses this URI for routing mobile terminated requests.

P-Charging-Vector: The S-CSCF stores the contents of the icid parameters for possible charging activities.

18. **Authentication**

Upon receiving an integrity protected REGISTER request carrying the authentication challenge response, the S-CSCF checks that the expected response (calculated by the S-CSCF using XRES and other parameter as defined in RFC 3310 [18]) matches the received challenge response. If the check is successful then the user has been authenticated and the public user identity is registered in the S-CSCF.

19. **Cx: S-CSCF registration notification procedure**

On registering a user the S-CSCF informs the HSS that the user has been registered at this instance. Upon being requested by the S-CSCF , the HSS will also include the user profile in the response sent to the S-CSCF.

For detailed message flows see 3GPP TS 29.228.

Table 6.2-19a provides the parameters in the REGISTER request (flow 17), which are sent to the HSS.

Table 6.2-19a Cx: S-CSCF registration notification procedure (S-CSCF to HSS)

Message source & destination	Cx Information element name	Information Source in REGISTER	Description
S-CSCF to HSS	Public User Identify	To:	Identity which is used to communicate with other users
	Private User Identity	Authorization:	The Private User Identity is encoded in the username field according to the Authorization protocol.
	S-CSCF name	Request-URI:	This information indicates the serving CSCF's name of that user

20. **200 OK response (S-CSCF to I-CSCF) - see example in table 6.2-20**

The S-CSCF sends a 200 (OK) response to the I-CSCF indicating that Registration was successful.

Table 6.2-20: 200 OK response (S-CSCF to I-CSCF)

```
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
Path: <sip:term@pcscf1.visited1.net;lr>
Service-Route: <sip:orig@scscf1.home1.net;lr>
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:
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
P-Associated-URI: <sip:user1_public2@home1.net>, <sip:user1_public3@home1.net>, <sip:+1-212-
   555-1111@home1.net;user=phone>
Content-Length:
```

Service-Route: The S-CSCF inserts the Service-Route header that includes its own URI including a character string in the user part to differentiate mobile originating requests from mobile terminating requests.

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

21. **200 OK response (I-CSCF to P-CSCF) - see example in table 6.2-21**

The I-CSCF removes the P-Charging-Function-Addresses header, as P-CSCF is in a different network, prior to forwarding~~s~~ the 200 (OK) response from the S-CSCF to the P-CSCF indicating that the registration was successful.

Table 6.2-21: 200 OK response (I-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
Path:
Service-Route:
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

22. **200 OK response (P-CSCF to UE) - see example in table 6.2-22**

The P-CSCF saves the value of the Service-Route header and associates it with the UE. The P-CSCF then forwards the 200 (OK) response from the I-CSCF to the UE indicating that the registration was successful.

Table 6.2-22: 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Path:
Service-Route:
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

XXXXXXXXXXXXXXXXXXXXXX NEXT CHANGES XXXXXXXXXXXXXXXXXXXXX

6.3 Registration signalling: reregistration - user currently registered

For the purpose of the reregistration signalling flow shown in figure 6.3-1, the subscriber is considered to be roaming. The HSS information indicates that the subscriber is registered and authenticated, and that the S-CSCF has been allocated to this subscriber. In this signalling flow, the home network does not have network configuration hiding active. This flow also shows the authentication of the private user identity.

This signalling flow assumes:

1. That the same PDP Context allocated during the initial registration scenario is still used for reregistration. For the case when the UE does not still have an active PDP context then PDP context procedures from subclause 16.2 is completed first.

2. The DHCP procedure employed for P-CSCF discovery is not needed.

3. The S-CSCF selection procedure invoked by the I-CSCF is not needed.

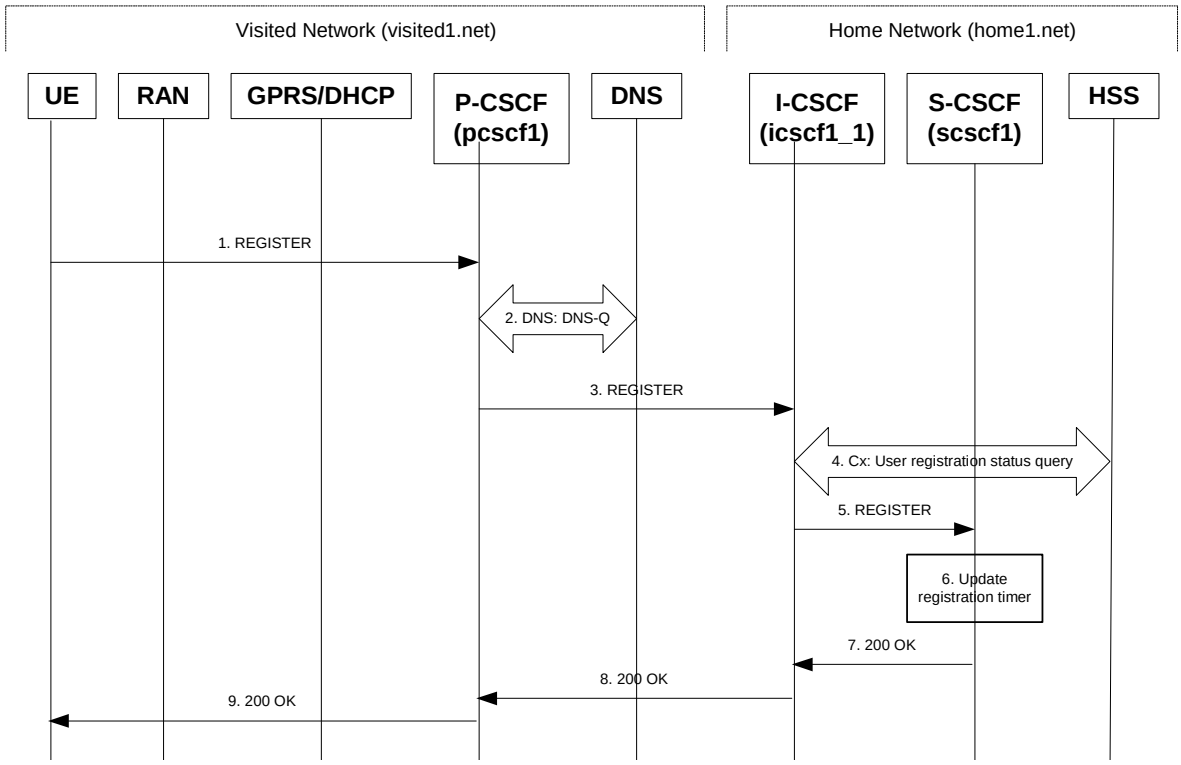

Figure 6.3-1: Reregistration when UE roaming

1. **REGISTER request (UE to P-CSCF) - see example in table 6.3-1**

The registration expires in the UE. The UE reregisters by sending a new REGISTER request. This request is sent to the same P-CSCF with which the UE initially registered.

Table 6.3-1: REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.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
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
   uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-
   protected="yes"
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-c=2468;
   port-s=1357
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
   c=8642; port-s=7531
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 3 REGISTER
Supported: path
Content-Length: 0
```

The header field usage is the same as for the initial registration scenario:

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

From: This indicates the public user identity originating the REGISTER request. The public user identity may be obtained from the USIM.

To: This indicates public user identity being registered. This is the identity by which other parties know this subscriber.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary identifier for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the S-CSCF.

Authorization: It carries authentication information. The private user identity (user1_private@home1.net) is carried in the username field of the Digest AKA protocol. As this is a re-registration process, the cached information (realm, nonce, algorithm, uri, response) is also sent.

NOTE 1: The actual nonce value in the WWW-Authenticate header field is encoded in base64, and it may look like: nonce="A34Cm+Fva37UYWpGNB34JP"

Security-Client: Lists the supported algorithm(s) by the UE. The values spi-c, spi-s, port-c and port-s are new parameter values and will not be used for security association setup in case the request is answered with 200 (OK).

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

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Supported: This header is included to indicate to the recipient that the UE supports the Path header.

Upon receiving this request the P-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

2. **DNS: DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs the DNS queries to locate the I-CSCF in the home network. The look up in the DNS is based on the domain name specified in the Request URI. The DNS provides the P-CSCF with the address of the I-CSCF in the home network. The P-CSCF must not use the I-CSCF address cached as a result of the previous registration.

3. **REGISTER request (P-CSCF to I-CSCF) - see example in table 6.3-3**

This signalling flow shows the REGISTER request being forward from the P-CSCF to the I-CSCF in the home domain.

The P-CSCF removes the Security-Client 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 6.3-3 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.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
P-Access-Network-Info:
Max-Forwards: 69
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
   uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-
   protected="yes"
CSeq:
Supported:
Content-Length:
```

Path: This is the P-CSCF URI and is included to inform the S-CSCF where to route terminating requests.

Require: This header is included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

P-Visited-Network-ID: It contains the identifier of the P-CSCF network at the home network.

P-Charging-Vector: The P-CSCF inserts this header and populates the icid parameters with the same globally unique value that was used in the previous registration.

4. **Cx: User registration status query procedure**

The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. Because the user has registered, the HSS returns the I-CSCF with the S-CSCF address for the subscriber.

For detailed message flows see 3GPP TS 29.228.

For the parameters in the REGISTER request (flow 3) which need to be sent to HSS, see table 6.2-5a.

Table 6.3-4a provides the parameters in the REGISTER request (flow 5), which are obtained from the information sent back from the HSS.

Table 6.3-4a Cx: User registration status query procedure (HSS to I-CSCF)

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

5. **REGISTER request (I-CSCF to S-CSCF) - see example in table 6.3-5**

This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

Table 6.3-5: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.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
P-Access-Network-Info:
Max-Forwards: 68
Path:
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Supported:
Content-Length:
```

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

Path: The S-CSCF stores the contents of the Path header and uses this URI for routing mobile terminated requests.

P-Visited-Network-ID: It contains the identifier of the P-CSCF network at the home network.

Upon receiving this request the S-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

6. **Update registration timer**

   As the REGISTER request arrived integrity protected, the S-CSCF does not need to challenge the user, but just update the registration timer to the value requested by the user (if the policy of the network allows it).

NOTE: The S-CSCF is allowed to challenge the user. If S-CSCF decides to challenge the user, the call flow will be similar to the one presented in section 6.2.

7. **200 OK response (S-CSCF to I-CSCF) – see example in Table 6.3-7**

   The S-CSCF sends a 200 (OK) response to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 6.3-7 200 OK response (S-CSCF to I-CSCF)

```
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
Path:
Service-Route: <sip:orig@scscf1.home1.net;lr>
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:
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
P-Associated-URI: <sip:user1_public2@home1.net>, <sip:user1_public3@home1.net>, <sip:+1-212-
   555-1111@home1.net;user=phone>
Content-Length:
```

Service-Route: The S-CSCF inserts the Service-Route header that includes its own URI including a character string in the user part to differentiate mobile originating requests from mobile terminating requests.

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

8. **200 OK response (I-CSCF to P-CSCF) – see example in Table 6.3-8**

   The I-CSCF removes the P-Charging-Function-Addresses header, as P-CSCF is in a different network, prior to forwarding~~s~~ the 200 (OK) response from the S-CSCF to the P-CSCF indicating that the registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 6.3-8 200 OK response (I-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
Path:
Service-Route:
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

9. **200 OK response (P-CSCF to UE) – see example in Table 6.3-9**

   The P-CSCF saves the value of the Service-Route header and associates it with the UE. The P-CSCF then forwards 200 (OK) response from the I-CSCF to the UE indicating that the registration was successful.

Table 6.3-9 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Path:
Service-Route:
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

XXXXXXXXXXXXXXXXXXXXXX NEXT CHANGES XXXXXXXXXXXXXXXXXXXXX

16.2 Registration signalling: user not registered

Figure 16.2-1 shows the registration signalling flow for the scenario when the user is not registered. For the purpose of this signalling flow, the subscriber is considered to be roaming. This flow also shows the authentication of the private user identity. In this signalling flow, the home network has network configuration hiding active.

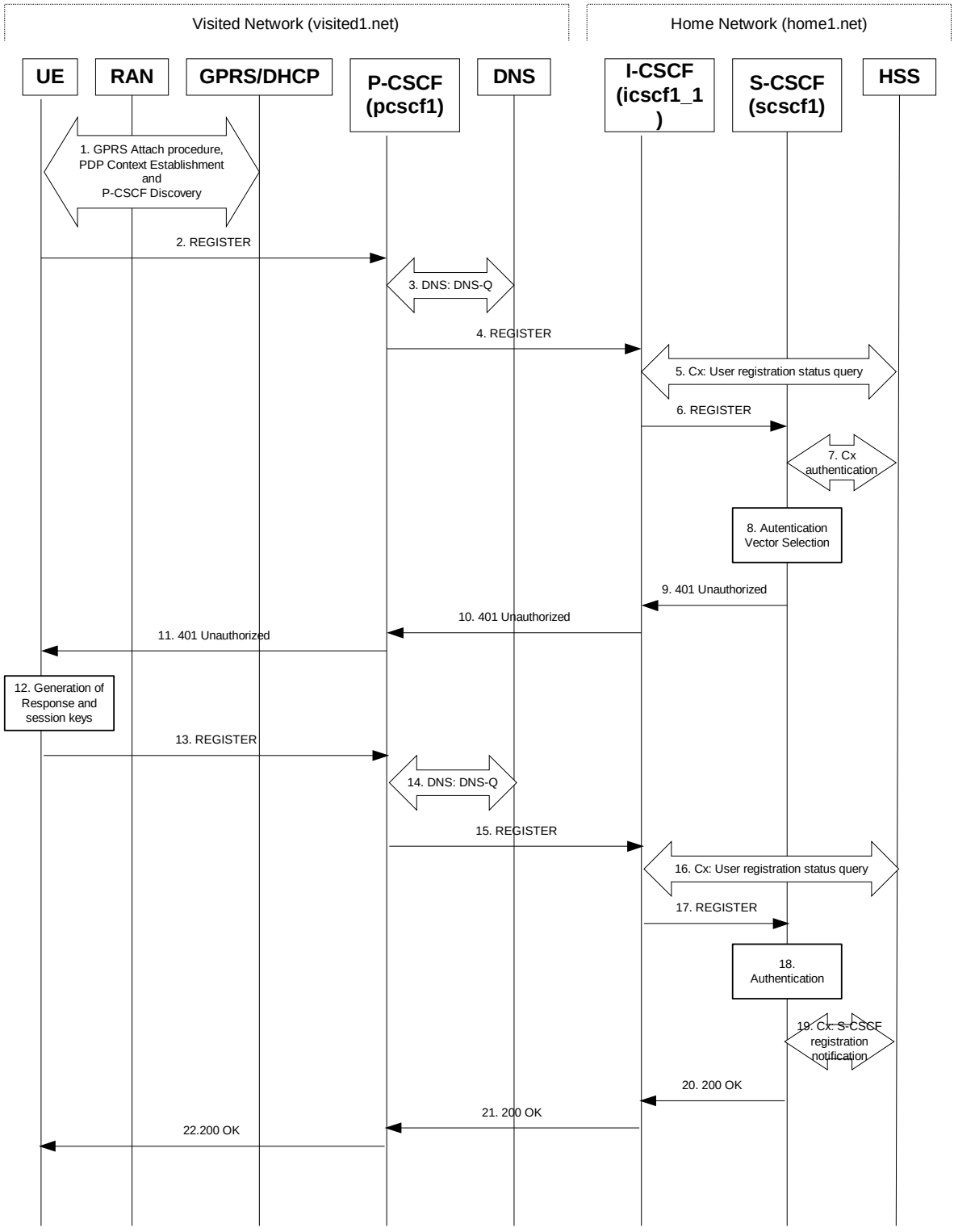

Figure 16.2-1: Registration when UE roaming

1. **GPRS Attach / PDP Context Establishment and P-CSCF Discovery (UE to GPRS)**

   This signalling flow is shown to indicate prerequisites for the registration signalling.

   See subclause 5.2 for details.

2. **REGISTER request (UE to P-CSCF) – see example in table 16.2-2**

The purpose of this request is to register the user's SIP URI with a S-CSCF in the home network. This request is routed to the P-CSCF because it is the only SIP server known to the UE.

Table 16.2-2 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11'
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd];comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce="", uri="sip:registrar.home1.net", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-c=2468;
   port-s=1357
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 1 REGISTER
Supported: path
Content-Length: 0
```

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("registrar.home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Via: IPv6 address of UE allocated during the PDP Context Activation process.

Max-Forwards: Set to 70 by the UE and used to prevent loops.

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

From: This indicates the public user identity originating the REGISTER request. The public user identity may be obtained from the USIM.

To: This indicates the public user identity being registered. This is the identity by which other parties know this subscriber. It may be obtained from the USIM.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary point of contact for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the S-CSCF.

Authorization: It carries authentication information. The private user identity (user1_private@home1.net) is carried in the username field of the Digest AKA protocol. The uri parameter (directive) contains the same value as the Request-URI. The realm parameter (directive) contains the network name where the username is authenticated. The Request-URI and the realm parameter (directive) value are obtained from the same field in the USIM, and therefore, are identical. In this example, it is assumed that a new UICC card was just inserted into the terminal, and there is no other cached information to send. Therefore, nonce and response parameters (directives) are empty.

Security-Client: Lists the supported algorithm(s) by the UE.

Supported: This header is included to indicate to the recipient that the UE supports the Path header.

Upon receiving this request the P-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

3. **DNS: DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs the DNS queries to locate the I-CSCF in the home network. The look up in the DNS is based on the domain name specified in the Request URI.

The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify a numeric IP address, and the transport protocol and port are not indicated, the P-CSCF performs an NAPTR query for the domain specified in the Request-URI.

Table 16.2-3a DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=registrar.home1.net, QCLASS=IN, QTYPE=NAPTR
```

The DNS records are retrieved according to RFC 3263 [14].

Table 16.2-3b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=registrar.home1.net,  QCLASS=IN, QTYPE=NAPTR

registrar.home1.net          0 IN NAPTR 50   50 "s" "SIP+D2U"    ""
     _sip._udp.registrar.home1.net
                      0 IN NAPTR 90   50 "s" "SIP+D2T"    ""  _sip._tcp.registrar.home1.net
                              0 IN NAPTR 100  50 "s" "SIPS+D2T"   ""
     _sips._tcp.registrar.home1.net
```

Based on the order and preference of the NAPTR record and the local preference, UDP is preferred and the P-CSCF finds the I-CSCF by a DNS SRV lookup according to RFC 2782 [4].

Table 16.2-3c DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=_sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

The DNS records are retrieved according to RFC 2782 [4].

Table 16.2-3d DNS: DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=_sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net        0 IN SRV 1 10 5060 icscf1_p.home1.com
                                     0 IN SRV 1  0 5060 icscf7_p.home1.com

icscf1_p.home1.net                       0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                       0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

4. **REGISTER request (P-CSCF to I-CSCF) – see example in table 16.2-4**

   The P-CSCF removes the Security-Client 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 P-CSCF needs to be in the path for all terminating requests for this user. To ensure this, the P-CSCF adds itself to the path for future requests.

   The P-CSCF adds also the P-Visited-Network-ID header with the contents of the identifier of the P-CSCF network. This may be the visited network domain name or any other identifier that identifies the visited network at the home network.

   This signalling flow shows the REGISTER request being forward from the P-CSCF to the I-CSCF in the home domain.

Table 16.2-4 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.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];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce="", uri="sip:registrar.home1.net", response="", integrity-protected="no"
CSeq:
Supported:
Content-Length:
```

Path: This is the address of the P-CSCF and is included to inform the S-CSCF where to route terminating requests.

Require: This header is included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

P-Visited-Network-ID: It contains the identifier of the P-CSCF network at the home network.

5. **Cx: User registration status query procedure**

   The I-CSCF makes a request for information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

   For detailed message flows see 3GPP TS 29.228.

   Table 6.2-5a provides the parameters in the REGISTER request (flow 4) which need to been sent to HSS.

6. **REGISTER request (I-CSCF to S-CSCF) – see example in table 16.2-6**

   I-CSCF adds a proper I-CSCF URI to the Path header.

   This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

Table 16.2-6 REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.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];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info:
Path: <sip:icscf1_p.home1.net;lr>, <sip:term@pcscf1.visited1.net;lr>
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Supported: path
Content-Length:
```

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

Path: The S-CSCF stores the contents of the Path header and uses these URIs for routing mobile terminated requests.

Upon receiving this request the S-CSCF will set it's SIP registration timer for this UE to the Expires time in this request.

7. **Cx: S-CSCF authentication procedure**

   As the REGISTER request arrived without integrity protection to the P-CSCF, the S-CSCF shall challenge it. For this, the S-CSCF requires at least one authentication vector to be used in the challenge to the user. If a valid AV is not available, then the S-CSCF requests at least one AV from the HSS.

   For detailed message flows see 3GPP TS 29.228.

   Table 6.2-7a provides the parameters in the REGISTER request (flow 6) which need to be sent to HSS.

8. **Authentication vector selection**

   The S-CSCF selects an authentication vector for use in the authentication challenge. For detailed description of the authentication vector, see 3GPP TS 33.203.

NOTE 1: The authentication vector may be of the form 3GPP TS 33.203 (if IMS AKA is the selected authentication scheme):

$AV = RAND_n||AUTN_n||XRES_n||CK_n||IK_n$ where:

- RAND: random number used to generate the XRES, CK, IK, and part of the AUTN. It is also used to generate the RES at the UE.
- AUTN: Authentication token (including MAC and SQN).
- XRES: Expected (correct) result from the UE.
- CK: Cipher key (optional).
- IK: Integrity key.

9. **401 Unauthorized response (S-CSCF to I-CSCF) – see example in table 16.2-9**

   The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 16.2-9: 401 Unauthorized response (S-CSCF to I-CSCF)

```
SIP/2.0 401 Unauthorized
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];comp=sigcomp;branch=z9hG4bKnashds7
From:
To: <sip:user1_public1@home1.net>;tag=5ef4
Call-ID:
WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN + server
   specific data), algorithm=AKAv1-MD5, ik="00112233445566778899aabbccddeeff",
   ck="ffeeddccbbaa11223344556677889900"
CSeq:
Content-Length:
```

WWW-Authenticate: The S-CSCF challenges the user. The nonce includes the quoted string, base64 encoded value of the concatenation of the AKA RAND, AKA AUTN and server specific data. The S-CSCF appends also the Integrity Key (IK) and the Cyphering key (CK).

NOTE: The actual nonce value in the WWW-Authenticate header field is encoded in base64, and it may look like: nonce="A34Cm+Fva37UYWpGNB34JP"

10. **401 Unauthorized response (I-CSCF to P-CSCF) – see example in table 16.2-10**

The authentication challenge is sent in the 401 Unauthorized response towards the UE.

Table 16.2-10: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
WWW-Authenticate:
CSeq:
Content-Length:
```

11. **401 Unauthorized response (P-CSCF to UE) – see example in table 16.2-11**

The P-CSCF removes any keys received in the 401 Unauthorized response and forwards the rest of the response to the UE.

Table 16.2-11: 401 Unauthorized response (P-CSCF to UE)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN + server
   specific data), algorithm=AKAv1-MD5
Security-Server: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
   c=8642; port-s=7531
CSeq:
Content-Length:
```

WWW-Authenticate: The P-CSCF removes the ik and ck parameters (directives) from the header.

12. **Generation of response and session keys at UE**

Upon receiving the Unauthorized response, the UE extracts the MAC and the SQN from the AUTN. The UE calculates the XMAC and checks that XMAC matches the received MAC and that the SQN is in the correct range. If both these checks are successful the UE calculates the response(using RES and other parameters as

defined in RFC 3310 [18]), and also computes the session keys IK and CK. The authentication challenge response is put into the Authorization header and sent back to the registrar in the REGISTER request.

13. **REGISTER request (UE to P-CSCF) – see example in table 16.2-13**

Table 16.2-13 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.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
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
   uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1"
Require: sec-agree
Proxy-Require: sec-agree
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-c=2468;
   port-s=1357
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: 2 REGISTER
Supported: path
Content-Length: 0
```

Authorization: This carries the response to the authentication challenge received in step 11 along with the private user identity , the realm, the nonce, the URI and the algorithm.

14. **DNS: DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs the DNS queries to locate the I-CSCF in the home network. The look up in the DNS is based on the domain name specified in the Request URI.

The P-CSCF sends the REGISTER request - after local processing - to the address indicated in the Request-URI. When forwarding the REGISTER request the P-CSCF needs to specify the protocol, port number and IP address of the I-CSCF server in the home network to which to send the REGISTER request. The P-CSCF tries to find this information by querying the DNS. Since the Request-URI does not specify a numeric IP address, and the transport protocol and port are not indicated, the P-CSCF performs an NAPTR query for the domain specified in the Request-URI.

Table 16.2-14a DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=registrar.home1.net, QCLASS=IN, QTYPE=NAPTR
```

The DNS records are retrieved according to RFC 3263 [14].

Table 16.2-14b DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=registrar.home1.net,  QCLASS=IN, QTYPE=NAPTR

registrar.home1.net          0 IN NAPTR 50   50 "s" "SIP+D2U"    ""
     _sip._udp.registrar.home1.net
                      0 IN NAPTR 90   50 "s" "SIP+D2T"    ""  _sip._tcp.registrar.home1.net
                              0 IN NAPTR 100  50 "s" "SIPS+D2T"   ""
     _sips._tcp.registrar.home1.net
```

Based on the order and preference of the NAPTR record and the local preference, UDP is preferred and the P-CSCF finds the I-CSCF by a DNS SRV lookup according to RFC 2782 [4].

Table 16.2-14c DNS: DNS Query (P-CSCF to DNS)

```
OPCODE=SQUERY
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV
```

The DNS records are retrieved according to RFC 2782 [4].

Table 16.2-14d DNS Query Response (DNS to P-CSCF)

```
OPCODE=SQUERY, RESPONSE, AA
QNAME=__sip._udp.registrar.home1.net, QCLASS=IN, QTYPE=SRV

_sip._udp.registrar.home1.net        0 IN SRV 1 10 5060 icscf1_p.home1.net
                                     0 IN SRV 1  0 5060 icscf7_p.home1.net

icscf1_p.home1.net                 0 IN AAAA     5555::aba:dab:aaa:daa
icscf7_p.home1.net                 0 IN AAAA     5555::a1a:b2b:c3c:d4d
```

In the Answer field of the query-response each I-CSCF is identified by its host domain name. The returned SRV Resource Records (RRs) are merged and ordered, and the selection technique (employing the Priority and Weight parameters returned in the RRs) as specified in RFC 2782 [4] is used to select the I-CSCF (i.e. the icscf1_p.home1.net). Since the Additional Data field of the query-response also contains the IP address of the selected I-CSCF (i.e. 5555::aba:dab:aaa:daa), a new query to the DNS is not required.

Once the IP address of the I-CSCF is obtained, the P-CSCF forwards the REGISTER request to this IP address (i.e. 5555::aba:dab:aaa:daa) using the UDP protocol and port number 5060.

15. **REGISTER request (P-CSCF to I-CSCF) – see example in table 16.2-15**

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.

This signalling flow shows the REGISTER request being forwarded from the P-CSCF to the I-CSCF in the home domain.

Table 16.2-15 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.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
P-Access-Network-Info:
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
   uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-
   protected="yes"
CSeq:
Supported:
Content-Length:
```

Path: This is the P-CSCF URI and is included to inform the S-CSCF where to route terminating requests.

16. **Cx: User registration status query procedure**

The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. The HSS returns the S-CSCF required capabilities and the I-CSCF uses this information to select a suitable S-CSCF.

For detailed message flows see 3GPP TS 29.228.

Table 6.2-16a provides the parameters in the REGISTER request (flow 15) which need to been sent to HSS.

17. **REGISTER request (I-CSCF to S-CSCF) – see example in table 16.2-17**

This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected.

Table 16.2-17 REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.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
P-Access-Network-Info:
Path: <sip:icscf1_p.home1.net;lr>, <sip:term@pcscf1.visited1.net;lr>
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Supported:
Content-Length:
```

Path: The I-CSCF adds an I-CSCF(THIG) to the list of URIs in the Path header. The S-CSCF stores the contents of the Path headers and uses these addresses for routing mobile terminated requests.

18. **Authentication**

Upon receiving an integrity protected REGISTER request, carrying the authentication challenge response, the S-CSCF checks that the expected response (calculated by the S-CSCF using XRES and other parameters as defined in RFC 3310 [18]) matches the received challenge response. If the check is successful then the user has been authenticated and the public user identity is registered in the S-CSCF.

19. **Cx: S-CSCF registration notification procedure**

On registering a user the S-CSCF informs the HSS that the user has been registered at this instance. The HSS stores the S-CSCF name for that subscriber. For a positive response, the HSS will include the user profile in the response sent to the S-CSCF.

For detailed message flows see 3GPP TS 29.228.

Table 6.2-19a provides the parameters in the SIP REGISTER request (flow 17) which need to been sent to HSS.

20. **200 OK response (S-CSCF to I-CSCF) – see example in table 16.2-20**

The S-CSCF sends a 200 (OK) response to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.2-20 200 OK response (S-CSCF to I-CSCF)

```
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
Path: <sip:icscf1_p.home1.net;lr>, <sip:term@pcscf1.visited1.net;lr>
Service-Route: <sip:icscf1_p.home1.net;lr>, <sip:orig@scscf1.home1.net;lr>
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:
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
P-Associated-URI: <sip:user1_public2@home1.net>, <sip:user1_public3@home1.net>, <sip:+1-212-
   555-1111@home1.net;user=phone>
Content-Length:
```

Service-Route: The S-CSCF inserts the Service-Route header that includes its own URI including a character string in the user part to differentiate mobile originating requests from mobile terminating requests.

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

21. **200 OK response (I-CSCF to P-CSCF) – see example in table 16.2-21**

The I-CSCF translates the S-CSCF name in the Service-Route header. The I-CSCF removes the P-Charging-Function-Addresses header, as it applies configuration hiding, prior to forwarding~~s~~ the 200 (OK) response from the S-CSCF to the P-CSCF indicating that the registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.2-21 200 OK response (I-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
Path:
Service-Route: <sip:icscf1_p.home1.net;lr>,
   <sip:token(orig@scscf1.home1.net;lr)@home1.net;tokenized-by=home1.net>
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

22. **200 OK response (P-CSCF to UE) – see example in table 16.2-22**

The P-CSCF saves the value of the Service-Route header and associates it with the UE. The P-CSCF then forwards the 200 (OK) response from the I-CSCF to the UE indicating the registration was successful.

Table 16.2-22 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Path:
Service-Route:
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

XXXXXXXXXXXXXXXXXXXXXX NEXT CHANGES XXXXXXXXXXXXXXXXXXXXX

16.3 Registration signalling: reregistration – user currently registered

For the purpose of the reregistration signalling flow shown in figure 16.3-1, the subscriber is considered to be roaming. This flow also shows the authentication of the private user identity. In this signalling flow, the home network has network configuration hiding active.

This signalling flow assumes:

1. That the same PDP Context allocated during the initial registration scenario is still used for reregistration. For the case when the UE does not still have an active PDP context then PDP context procedures from subclause 16.2 is completed first.

2. The S-CSCF selection procedure invoked by the I-CSCF is not needed.

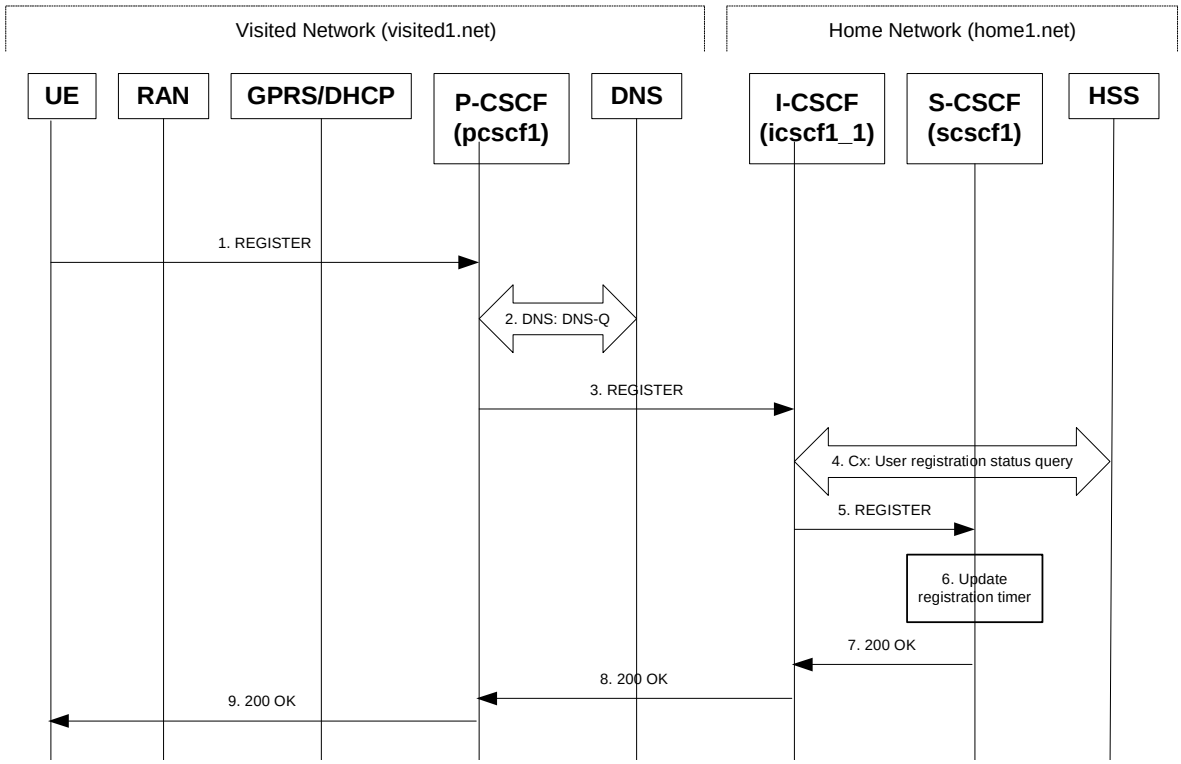

Figure 16.3-1: Reregistration when UE roaming

1. **REGISTER request (UE to P-CSCF) – see example in table 16.3-1**

   The registration expires in the UE. The UE reregisters by sending a new REGISTER request. This request is sent to the same P-CSCF with which the UE initially registered.

Table 16.3-1 REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.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
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
   uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1"
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678; port-c=2468;
   port-s=1357
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
   c=8642; port-s=7531
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 3 REGISTER
Supported: path
Content-Length: 0
```

The header field usage is the same as for the initial registration scenario:

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

From: This indicates the public user identity originating the REGISTER request. The public user identity may be obtained from the USIM.

To: This indicates public user identity being registered. This is the identity by which other parties know this subscriber.

Contact: This indicates the point-of-presence for the subscriber – the IP address of the UE. This is the temporary identifier for the subscriber that is being registered. Subsequent requests destined for this subscriber will be sent to this address. This information is stored in the P-CSCF.

Authorization: It carries authentication information. The private user identity (user1_private@home1.net) is carried in the username field of the Digest AKA protocol. As this is a re-registration process, the cached information (realm, nonce, algorithm, uri, response) is also sent.

NOTE 1: The actual nonce value in the WWW-Authenticate header field is encoded in base64, and it may look like: nonce="A34Cm+Fva37UYWpGNB34JP"

Request-URI: The Request-URI (the URI that follows the method name, "REGISTER", in the first line) indicates the destination domain of this REGISTER request. The rules for routing a SIP request describe how to use DNS to resolve this domain name ("home1.net") into an address or entry point into the home operator's network (the I-CSCF). This information is stored in the USIM.

Security-Client: Lists the supported algorithm(s) by the UE. The values spi-c, spi-s, port-c and port-s are new parameter values and will not be used for security association setup in case the request is answered with 200 (OK).

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

Supported: This header is included to indicate to the recipient that the UEsupports the Path header.

Upon receiving this request the P-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

2. **DNS: DNS-Q**

Based on the user's URI, the P-CSCF determines that UE is registering from a visiting domain and performs the DNS queries to locate the I-CSCF in the home network. The look up in the DNS is based on the address specified in the Request URI. The DNS provides the P-CSCF with an address of the I-CSCF in the home network. The P-CSCF must not use the I-CSCF address cached as a result of the previous registration.

3. **REGISTER request (P-CSCF to I-CSCF) – see example in table 16.3-3**

This signalling flow shows the REGISTER request being forward from the P-CSCF to the I-CSCF in the home domain.

The P-CSCF removes the Security-Client 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 16.3-3 REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.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
P-Access-Network-Info:
Max-Forwards: 69
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net", realm="registrar.home1.net",
   nonce=base64(RAND + AUTN + server specific data), algorithm=AKAv1-MD5,
   uri="sip:registrar.home1.net", response="6629fae49393a05397450978507c4ef1", integrity-
   protected="yes"
CSeq:
Supported: path
Content-Length:
```

Path: This is the P-CSCF URI and is included to inform the S-CSCF where to route terminating requests.

Require: This header is included to ensure that the recipient correctly handles the Path header. If the recipient does not support the path header, a response will be received with a status code of 420 and an Unsupported header indicating "path". Such a response indicates a misconfiguration of the routing tables and the request has been routed outside the IM CN subsystem.

P-Visited-Network-ID: It contains the identifier of the P-CSCF network at the home network.

4. **Cx: User registration status query procedure**

The I-CSCF requests information related to the Subscriber registration status by sending the private user identity, public user identity and visited domain name to the HSS. Because the user has registered, the HSS returns the I-CSCF with the S-CSCF address for the subscriber

For detailed message flows see 3GPP TS 29.228.

For the parameters in the REGISTER request (flow 3), which are sent to the HSS, see table 6.2-5a.

Table 6.3-4a provides the parameters in the SIP REGISTER request (flow 5), which are obtained from the information sent back from the HSS.

5. **REGISTER request (I-CSCF to S-CSCF) – see example in table 16.3-5**

This signalling flow forwards the REGISTER request from the I-CSCF to the S-CSCF selected. The Request-URI is changed to the address of the S-CSCF.

I-CSCF adds a proper I-CSCF name to the Path header.

Table 16.3-5 REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.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
P-Access-Network-Info:
Max-Forwards: 68
Path: <sip:icscf1_p.home1.net;lr>, <sip:term@pcscf1.visited1.net;lr>
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Authorization:
Call-ID:
CSeq:
Supported:
Content-Length:
```

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

Path: The S-CSCF stores the contents of the Path header and uses these URIs for routing mobile terminated requests.

P-Visited-Network-ID: It contains the identifier of the P-CSCF network at the home network.

Upon receiving this request the S-CSCF will detect that it already has a registration record for this UE and will reset it's SIP registration timer for this UE to the Expires time in this request.

6. **Update registration timer**

   As the REGISTER request arrived integrity protected, the S-CSCF does not need to challenge the user, but just update the registration timer to the value requested by the user (if the policy of the network allows it).

NOTE: The S-CSCF is allowed to challenge the user. If S-CSCF decides to challenge the user, the call flow will be similar to the one presented in section 16.2.

7. **200 OK response (S-CSCF to I-CSCF) – see example in Table 16.3-7**

   The S-CSCF sends a 200 (OK) response to the I-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.3-7 200 OK response (S-CSCF to I-CSCF)

```
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
Path: <sip:icscf1_p.home1.net;lr>, <sip:term@pcscf1.visited1.net;lr>
Service-Route: <sip:icscf1_p.home1.net;lr>, <sip:orig@scscf1.home1.net;lr>
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:
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
P-Associated-URI: <sip:user1_public2@home1.net>, <sip:user1_public3@home1.net>, <sip:+1-212-
   555-1111@home1.net;user=phone>
Content-Length:
```

Service-Route: The S-CSCF inserts the Service-Route header value that includes a URI of an I-CSCF (THIG) and its own URI including a character string in the user part to differentiate mobile originating requests from mobile terminating requests.

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

8. **200 OK response (I-CSCF to P-CSCF) – see example in Table 16.3-8**

   The I-CSCF translates the S-CSCF name in the Service-Route header. The I-CSCF removes the P-Charging-Function-Addresses header, as it applies configuration hiding, prior to forwarding~~s~~ the 200 (OK) response from the S-CSCF to the P-CSCF indicating that Registration was successful. This response will traverse the path that the REGISTER request took as described in the Via list.

Table 16.3-8 200 OK response (I-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
Path:
Service-Route: <sip:icscf1_p.home1.net;lr>,
   <sip:token(scscf1.home1.net;lr)@home1.net;tokenized-by=home1.net>
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

9. **200 OK response (P-CSCF to UE) – see example in Table 16.3-9**

   The P-CSCF saves the value of the Service-Route header and associates it with the UE. The P-CSCF then forwards the 200 (OK) response from the I-CSCF to the UE indicating the registration was successful.

Table 16.3-9 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Path:
Service-Route:
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

XXXXXXXXXXXXXXXXXXXXXX END of CHANGES XXXXXXXXXXXXXXXXXXXXX

3GPP TSG CN WG1 Meeting #33 **N1-040335**
Atlanta, USA, 16th – 20st February 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.228** **CR** **128** ⌘ **rev** **-** ⌘ Current version: **5.7.0** ⌘

*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 **X**

Title:	⌘	Editorial modification in notation conventions
Source:	⌘	Huawei, China Mobile
Work item code:	⌘	IMS-CCR
Date:	⌘	04/02/2004
Category:	⌘	**F**
Release:	⌘	REL-5

Use one of the following categories:
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.

Use one of the following releases:
2 (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)

Reason for change:	⌘	As a part of the TS 24.228, the clause “notation conventions” is necessary to the understanding of the whole specification, so the editorial errors found in the notation defination should be corrected.
Summary of change:	⌘	Miscellaneous corrections to the “notation conventions” subclause.
Consequences if not approved:	⌘	Many copy errors exist.

Clauses affected:	⌘	4.2.3			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	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.

4.2 Notation conventions

4.2.1 Introduction

This subclause details the notation conventions used in the present document.

4.2.2 User Identities

UE#1's public user identities are:

user1_public1@home1.net

user1_public2@home1.net

etc.

UE#1's private user identity is:

user1_private@home1.net

UE#2's public user identities are:

user2_public1@home2.net

user2_public2@home2.net

etc.

UE#2's private user identity is:

user2_private@home2.net

4.2.3 Network Entities

a) UE#1's associated entities:

UE#1's home network is:

home1.net

The P-CSCF serving UE#1 in home1.net is:

pcscf1.home1.net

The S-CSCF serving UE#1 is:

scscf1.home1.net

The I-CSCF in UE#1's home network (between proxy and serving CSCF) is:

icscf1_p.home1.net

If there are two I-CSCFs in home1.net involved in the call flows, then they are (from the left side of the individual call flow to its right side):

icscf1_p.home1.net

icscf1_s.home1.net

NOTE 1: Typically, the second I-CCSF will be between two S-CSCFs (hence use of "s").

UE#1 is roaming in:

visited1.net

The P-CSCF serving UE#1 in visited1.net is:

pcscf1.visited1.net

The BGCF serving UE#1 is:

bgcf1.home1.net

The MGCF serving UE#1 is:

mgcf1.home1.net

b) UE#2's associated entities (where UE#2's home and/or visited network is different from that of UE#1):

UE#2's home network is:

home2.net

The P-CSCF serving UE#2 in home2.net is:

pcscf2.home2.net

The S-CSCF serving UE#2 is:

scscf2.home2.net

The I-CSCF in UE#2's home network (between proxy and serving CSCF) is:

icscf2_p.home2.net

If there are two I-CSCFs in home2.net involved in the call flows, then they are (from the left side of the individual call flow to its right side):

icscf2_~~s~~p.home~~1~~2.net

icscf2_~~p~~s.home~~1~~2.net

NOTE 2: Typically, the second I-CCSF will be between two S-CSCFs (hence use of "s").

UE#2 is roaming in:

visited2.net

The P-CSCF serving UE#2 in visited2.net is:

pcscf2.visited2.net

The BGCF serving UE#~~1~~2 is:

bgcf2.home2.net

The MGCF serving UE#~~1~~2 is:

mgcf2.home2.net

c) UE#2's associated entities (where UE#2's home and/or visited network is the same as that of UE#1):

UE#2's home network is:

home1.net

The P-CSCF serving UE#2 in home1.net is:

pcscf2.home1.net

The S-CSCF serving UE#2 is:

scscf2.home1.net

The I-CSCF in UE#2's home network (between proxy and serving CSCF) is:

icscf2_p.home1.net

If there are two ~~UE#2~~ I-CSCFs involved in the call flows, then they are (from the left side of the individual call flow to its right side):

icscf2_~~s~~p.home1.net

icscf2_~~p~~s.home1.net

NOTE 3: Typically, the second I-CCSF will be between two S-CSCFs (hence use of "s").

UE#2 is roaming in:

visited1.net

The P-CSCF serving UE#2 in visited2.net is:

pcscf2.visited1.net

The BGCF serving UE#~~1~~2 is:

bgcf2.home1.net

The MGCF serving UE#~~1~~2 is:

mgcf2.home1.net

d) UE#3's (i.e. target in call transfer scenario) associated entities (where UE#3's home and/or visited network is different from that of UE#1and UE#2):

If there is a Call Transfer, then the Transfer Target is UE#3

UE#3's home network is:

home3.net

The S-CSCF serving UE#3 is:

scscf3.home3.net

The I-CSCF in UE#3's home network (between proxy and serving CSCF) is:

icscf3_p.home3.net

If there are two I-CSCFs in home3.net involved in the call flows, then they are (from the left side of the individual call flow to its right side):

icscf3_~~s~~p.home3.net

icscf3_~~p~~s.home3.net

NOTE 4: Typically, the second I-CCSF will be between two S-CSCFs (hence use of "s").

UE#3 is roaming in:

visited3.net

The P-CSCF serving UE#3 in visited3.net is:

pcscf3.visited3.net

The BGCF serving UE#~~1~~3 is:

bgcf3.home3.net

The MGCF serving UE#~~1~~3 is:

mgcf3.home3.net