**3GPP TSG-CT WG1 Meeting #126-eC1-206457**

**Electronic meeting, 15-23 October 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.229** | **CR** | **6450** | **rev** | **2** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | 24.229 MPS Editors notes removal | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Perspecta Labs, CISA ECD, AT&T | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | MPS2 | | | | |  | ***Date:*** | | | 20-10-07 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change 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](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | UE initiated priority upgrades via P-CSCF need not be supported. Editor's notes related to how changed priority is signalled to network elements can be removed. The mechanism by which network elements are signalled priority is already defined elsewhere in TS 24.229. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Editor's notes were added to TS 24.229 because agreement could not be reached regarding how a UE could directly signal priority upgrades to the P-CSCF to satisfy the TS 22.153 requirement:  The system shall support means for a Service User using a UE with an MPS subscription to:  - …  - request upgrade of an established MMTEL video call, or an established MMTEL video conference call to MPS.  Network elements can request MPS upgrades. For example, an AS can modify the priority of a dialog. In TS 24.229, clause 5.7.2: "If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the AS shall include the Resource-Priority header field in all requests associated with that dialog."  Removed Editor's Notes related to how changed priority is signalled to the P-CSCF.  Added note to AS clauses: "How a UE can initiate a priority upgrade request via an AS is out of scope of this release of the specification." | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Editor’s notes remain in the specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.2.1, 5.3.2.1A, 5.4.3.2, 5.4.3.3, 5.5.1, 5.6.1, 5.7.2, 5.7.3, 5.8.1, 5.8A, 5.10.2.1A, 5.13.2.2, I.1A | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\*\*\*\*\* First change \*\*\*\*\*

#### 5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for initial requests.

Upon receipt of a request, the I-CSCF shall perform the originating procedures as described in subclause 5.3.2.1A if the topmost Route header field of the request contains the "orig" parameter. Otherwise, the I-CSCF shall continue with the rest of the procedures of this subclause.

When the I-CSCF receives a request, the I-CSCF shall verify whether it has arrived from a trusted domain or not. If the request has arrived from a non trusted domain, then the I-CSCF shall remove all P-Charging-Vector header fields and all P-Charging-Function-Addresses header fields the request may contain.

NOTE 1: The I-CSCF can find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the I-CSCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the I-CSCF shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE 2: The special treatment can included filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

The I-CSCF shall discard the P-Profile-Key header field, if the I-CSCF receives the P-Profile-Key header field in a SIP request or response.

When the I-CSCF receives, destined for a served user or a PSI, an initial request for a dialog or standalone transaction the I-CSCF shall:

1) if the Request-URI includes:

a) a pres: or an im: URI, then translate the pres: or im: URI to a public user identity and replace the Request-URI of the incoming request with that public user identity; or

b) a SIP-URI that is not a GRUU and with the user part starting with a + and the "user" SIP URI parameter equals "phone" then replace the Request-URI with a tel-URI with the user part of the SIP-URI in the telephone-subscriber element in the tel-URI, and carry forward the tel-URI parameters that may be present in the Request-URI; or

c) a SIP URI that is a GRUU, then obtain the public user identity or an identity of the UE that represents the functionality within the UE that performs the role of registrar from the Request-URI and use it for location query procedure to the HSS. When forwarding the request, the I-CSCF shall not modify the Request-URI of the incoming request;

NOTE 3: SRV records have to be advertised in DNS pointing to the I-CSCF for pres: and im: queries.

2) remove its own SIP URI from the topmost Route header field, if present; and

3) check if the domain name of the Request-URI matches with one of the PSI subdomains configured in the I-CSCF. If the match is successful, the I-CSCF resolves the Request-URI by an internal DNS mechanism into the IP address of the AS hosting the PSI and does not start the user location query procedure. Otherwise, the I-CSCF will start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called PSI or user, indicated in or derived from the Request-URI. Prior to performing the user location 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].

When the I-CSCF receives any response to such a request, the I-CSCF shall store the value of the "term-ioi" header field parameter received in the P-Charging-Vector header field, if present.

NOTE 4: A received "term-ioi" header field parameter will be a type 3 IOI if received from an AS hosting a PSI or a type 2 IOI if received from the S-CSCF of the served user. The type 3 IOI identifies the service provider from which the response was sent and the type 2 IOI identifies the network from which the response was sent.

When the I-CSCF receives an INVITE request, the I-CSCF may require the periodic refreshment of the session to avoid hung states in the I-CSCF. If the I-CSCF requires the session to be refreshed, then the I-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 5: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

In case the I-CSCF is able to resolve the Request-URI into the IP address of the AS hosting the PSI, then the I-CSCF shall:

1) store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field. If no P-Charging-Vector header field was found, then insert the P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17]. The I-CSCF shall insert a type 3 "orig-ioi" header field parameter in place of any received "orig-ioi" header field parameter. The I-CSCF shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The I-CSCF shall not include the type 3 "term-ioi" header field parameter. Based on local policy, the I-CSCF shall add an "fe-addr" element of the "fe-identifier" header field parameter to the P-Charging-Vector header field with its own address or identifier; and

2) forward the request directly to the AS hosting the PSI.

Upon successful user location query, when the response contains the URI of the assigned S-CSCF, or the URI of an AS hosting the PSI, the I-CSCF shall:

1) insert the URI received from the HSS as the topmost Route header field;

2) store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the P-Charging-Vector header field in the P-Charging-Vector header field. If no "icid-value" header field parameter was found, then insert the P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17];

2A) based on local policy, add an "fe-addr" element of the "fe-identifier" header field parameter to the P-Charging-Vector header field with its own address or identifier;

3) optionally, include the received Redirect-Host AVP value in the P-User-Database header field as defined in RFC 4457 [82];

3A) if the Wildcarded Identity value is received from the HSS in the Wildcarded-Identity AVP and the I-CSCF supports the SIP P-Profile-Key private header extension, include the wildcarded identity value in the P-Profile-Key header field as defined in RFC 5002 [97]; and

4) forward the request based on the topmost Route header field.

NOTE 6: The P-User-Database header field can be included only if the I-CSCF can assume (e.g. based on local configuration) that the receiving S-CSCF will be able to process the header field.

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

1) if overlap signalling using the multiple-INVITEs method is supported as a network option, and if the I-CSCF receives an INVITE request outside an existing dialog with the same Call ID and From header as a previous INVITE request during a certain period of time, route the new INVITE to the same next hop as the previous INVITE request; otherwise

2) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];

3) insert the URI of the selected S-CSCF as the topmost Route header field value;

4) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URI of the assigned S-CSCF);

5) optionally, include the received Redirect-Host AVP value in the P-User-Database header field as defined in RFC 4457 [82];

6) if the Wildcarded Identity value is received from the HSS in the Wildcarded-Identity AVP and the I-CSCF supports the SIP P-Profile-Key private header extension, include the wildcarded identity value in the P-Profile-Key header field as defined in RFC 5002 [97]; and

NOTE 7: A Wildcarded Identity can be either a PSI or a public user identity.

7) forward the request to the selected S-CSCF.

NOTE 8: The P-User-Database header field can be included only if the I-CSCF can assume (e.g. based on local configuration) that the receiving S-CSCF will be able to process the header field.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, and if the Request-URI is a tel URI containing a public telecommunications number as specified in RFC 3966 [22], the I-CSCF may support a local configuration option that indicates whether or not request routeing is to be attempted. If the local configuration option indicates that request routeing is to be attempted, then the I-CSCF shall perform one of the following procedures based on local operator policy:

1) forward the request to the transit functionality for subsequent routeing; or

2) invoke the portion of the transit functionality that translates the public telecommunications number contained in the Request-URI to a routeable SIP URI, and process the request based on the result, as follows:

a) if the translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g. a MRFC to play an announcement) in the home network, or the I-CSCF may send an appropriate SIP response to the originator, such as 404 (Not Found) or 604 (Does not exist anywhere). When forwarding the request to a BGCF or any other appropriate entity, the I-CSCF shall leave the original Request-URI containing the tel URI unmodified:

i) if overlap signalling using the multiple-INVITEs method is supported as a network option, and if the I-CSCF receives an INVITE request outside an existing dialog with the same Call ID and From header as a previous INVITE request during a certain period of time, the I-CSCF shall route the new INVITE to the same next hop as the previous INVITE request; and

ii) additional procedures apply if the I-CSCF supports NP capabilities and these capabilities are enabled by local policy, and the database used for translation from an international public telecommunications number to a SIP URI also provides NP data (for example, based on the PSTN Enumservice as defined by RFC 4769 [114] or other appropriate data bases). If the above translation from an international public telecommunications number to a SIP URI failed, but NP data was obtained from the database, then the I-CSCF shall replace the tel-URI in the Request-URI with the obtained NP data, prior to forwarding the request to the BGCF or other appropriate entity. The URI is updated by the I-CSCF by adding the NP parameters defined by RFC 4694 [112] to the tel-URI in the Request-URI: an "npdi" tel-URI parameter is added to indicate that NP data retrieval has been performed, and if the number is ported, an "rn" tel-URI parameter is added to identify the ported-to routeing number. The I-CSCF shall perform these procedures if the tel-URI in the received Request-URI does not contain an "npdi" tel-URI parameter. In addition, the I-CSCF may, based on local policy, perform these procedures when the tel-URI in the received Request-URI contains an "npdi" tel-URI parameter indicating that the NP data has been previously obtained; or

NOTE 9: The I-CSCF might need to replace NP data added by a previous network if the previous network's NP database did not contain the local ported data for the called number. When the I-CSCF replaces the tel URI in the Request-URI with the obtained NP data, all tel URI parameters in the received Request-URI will be replaced by the obtained NP data.

b) if this translation succeeds, then replace the Request-URI with the routeable SIP URI and process the request as follows:

- determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header field if present, otherwise based on the Request-URI. If the destination requires interconnect functionalities (e.g. the destination address is of an IP address type other than the IP address type used in the IM CN subsystem), the I-CSCF shall:

i) if the I-CSCF supports indicating the traffic leg as specified in RFC 7549 [225] and required by local policy, append the "iotl" SIP URI parameter set to "homeA-homeB" to the Request-URI; and

ii) forward the request to the destination address via an IBCF in the same network;

- if network hiding is needed due to local policy, put the address of the IBCF to the topmost Route header field;

- route the request based on SIP routeing procedures; and

- if overlap signalling using the multiple-INVITE method is supported as a network option, and if the I-CSCF receives an INVITE request outside an existing dialog with the same Call ID and From header as a previous INVITE request during a certain period of time, route the new INVITE to the same next hop as the previous INVITE request.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, and if local operator policy does not indicate that request routeing is to be attempted, then, the I-CSCF shall return an appropriate unsuccessful SIP response. Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, and if if the Request-URI is a SIP URI, the I-CSCF shall also return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) response if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that contains a single Route header field pointing to itself, the I-CSCF shall determine from the entry in the Route header field whether it needs to do HSS query. In case HSS query not is needed, then the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header field; and

2) route the request based on the Request-URI.

When the I-CSCF receives an initial request for a dialog or standalone transaction containing more than one Route header field, the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header field; and

2) forward the request based on the topmost Route header field.

NOTE 10: In accordance with SIP the I-CSCF can add its own routeable SIP URI to the top of the Record-Route header field to any request, independently of whether it is an initial request. The P-CSCF will ignore any Record-Route header field that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 (Session Progress) response or 2xx response), the I-CSCF shall store the values from the P-Charging-Function-Addresses header field, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header field prior to forwarding the message.

When the I-CSCF receives any response to the initial request for a dialog or standalone transaction containing a "term-ioi" header field parameter in the P-Charging-Vector header field from the AS hosting the PSI, the I-CSCF shall:

1) remove all received "orig-ioi" and "term-ioi" header field parameters from the forwarded response;

2) insert the stored "orig-ioi" header field parameter if received in the request; and

3) insert a type 2 "term-ioi" header field parameter. The "term-ioi" header field parameter is set to a value that identifies the sending network of the response.

When the I-CSCF, upon sending an initial INVITE request to the S-CSCF, receives a 305 (Use Proxy) response from the S-CSCF, the I-CSCF shall forward the initial INVITE request to the SIP URI indicated in the Contact field of the 305 (Use Proxy) response, as specified in RFC 3261 [26].

\*\*\*\*\* Second change \*\*\*\*\*

#### 5.3.2.1A Originating procedures for requests containing the "orig" parameter

The procedures of this subclause apply for requests received at the I-CSCF when the topmost Route header field of the request contains the "orig" parameter.

The I-CSCF shall verify for all requests whether they arrived from a trusted domain or not. If the request arrived from a non trusted domain, then the I-CSCF shall respond with 403 (Forbidden) response.

If the request arrived from a trusted domain, the I-CSCF shall perform the procedures below.

NOTE 1: The I-CSCF can find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the I-CSCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the I-CSCF shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE 2: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

If the I-CSCF receives the P-Profile-Key header field in a SIP request or response the I-CSCF shall discard the P-Profile-Key header field.

When the I-CSCF receives an initial request for a dialog or standalone transaction the I-CSCF will start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the calling user, indicated in either:

1) the P-Served-User header field, if included in the request; or

2) the P-Asserted-Identity header field, if the P-Served-User header field is not included in the request.

Prior to performing the user location 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].

When the I-CSCF receives an INVITE request, the I-CSCF may require the periodic refreshment of the session to avoid hung states in the I-CSCF. If the I-CSCF requires the session to be refreshed, the I-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 3: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

When the response for user location query contains information about the required S-CSCF capabilities, the I-CSCF shall select a S-CSCF according to the method described in 3GPP TS 29.228 [14].

If the user location query was successful, the I-CSCF shall:

1) insert the URI of an AS hosting the PSI, or the URI of the S-CSCF - either received from the HSS, or selected by the I-CSCF based on capabilities - as the topmost Route header field appending the "orig" parameter to the URI of the S-CSCF;

2) store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field. If no P-Charging-Vector header field was found, then insert the P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17];

2A) based on local policy, add an "fe-addr" element of the "fe-identifier" header field parameter to the P-Charging-Vector header field with its own address or identifier;

3) optionally, include the received Redirect-Host AVP value in the P-User-Database header field as defined in RFC 4457 [82];

4) if a wildcarded identity value is received from the HSS in the Wildcarded-Identity AVP and the I-CSCF supports the SIP P-Profile-Key private header extension, include the wildcarded public user identity value in the P-Profile-Key header field as defined in RFC 5002 [97]; and

5) forward the request based on the topmost Route header field.

NOTE 4: The P-User-Database header field can be included only if the I-CSCF can assume (e.g. based on local configuration) that the receiving S-CSCF will be able to process the header field.

Upon an unsuccessful user location query, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) response or 604 (Does not exist anywhere) response in the case the user is not a user of the home network.

When the I-CSCF receives any response to the above request, and forwards it to AS, the I-CSCF shall:

- store the values from the P-Charging-Function-Addresses header field, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header field prior to forwarding the message; and

- insert a P-Charging-Vector header field containing the type 3 "orig-ioi" header field parameter, if received in the request, and a type 3 "term-ioi" header field parameter in the response. The I-CSCF shall set the type 3 "term-ioi" header field parameter to a value that identifies the sending network of the response and the type 3 "orig-ioi" header field parameter is set to the previously received value of type 3 "orig-ioi" header field parameter.

\*\*\*\*\* Third change \*\*\*\*\*

#### 5.4.3.2 Requests initiated by the served user

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the S-CSCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the S-CSCF shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE 1: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the S-CSCF receives from the UE an initial request for a dialog, which contains a GRUU and an "ob" SIP URI parameter in the Contact header field, and multiple contact addresses have been registered for the specific GRUU, then for all subsequent in-dialog requests sent toward the UE's, the S-CSCF shall populate the Request-URI with the registered contact address from which the UE sent the initial request for the dialog.

NOTE 2: When a given contact address is registered, the S-CSCF can use a dedicated value in its Service-Route header field entry to identify the given contact address. When the S-CSCF receives an initial request for a dialog, the S-CSCF can find out from which contact address the initial request was sent by looking at the preloaded Route header field (constructed from the Service-Route header field returned in the response for the REGISTER request) which contains the entry of the S-CSCF.

When performing SIP digest without TLS, when the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, the S-CSCF may perform the steps in subclause 5.4.3.6 to challenge the request based on local policy.

NOTE 3: If the user registration is associated with the state "tls-protected", then the execution of Proxy-Authorization as described in subclause 5.4.3.6 is still possible, although it is unlikely this would add additional security provided the P-CSCF is trusted. Thus, in most cases the state "tls-protected" will be reason for the S-CSCF to not desire Proxy-Authentication for this user.

NOTE 4: The option for the S-CSCF to challenge the request does not apply to a request from an AS acting as an originating UA.

When performing GPRS-IMS-Bundled authentication, when the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall check whether a "received" header field parameter exists in the Via header field provided by the UE. If a "received" header field parameter exists, S-CSCF shall compare the (prefix of the) IP address received in the "received" header field parameter against the UE's IP address (or prefix) stored during registration. If no "received" header field parameter exists in the Via header field provided by the UE, then S-CSCF shall compare the (prefix of the) IP address received in the "sent-by" parameter against the IP address (or prefix) stored during registration. If the stored IP address (or prefix) and the (prefix of the) IP address in the "received" Via header field parameter provided by the UE do not match, the S-CSCF shall reject the request with a 403 (Forbidden) response. In case the stored IP address (or prefix) and the (prefix of the) IP address in the "received" Via header field parameter provided by the UE do match, the S-CSCF shall proceed as described in the remainder of this subclause.

If the S-CSCF supports HSS based P-CSCF restoration, and receives a request from a P-CSCF that the S-CSCF considers is not reachable, the S-CSCF shall consider this P-CSCF as being reachable.

If the S-CSCF supports PCRF based P-CSCF restoration, and receives a request from a P-CSCF that the S-CSCF considers is in a not reachable, the S-CSCF shall consider this P-CSCF as being reachable.

When the S-CSCF receives from the served user or from a PSI an initial request for a dialog or a request for a standalone transaction, and the request is received either from a functional entity within the same trust domain or contains a valid original dialog identifier (see step 3) or the dialog identifier (From, To and Call-ID header fields) relates to an existing request processed by the S-CSCF, then prior to forwarding the request, the S-CSCF shall:

0) if the request is received from a P-CSCF that does not support the trust domain handling of the P-Served-User header field then remove any P-Served-User header fields;

1) determine the served user as follows:

a) if the request contains a P-Served-User header field then

i) determine the served user by taking the identity contained in a P-Served-User header field as defined in RFC 5502 [133]. Then check whether the determined served user is a barred public user identity. In case the said header field contains the served user identity is a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, the S-CSCF shall save the public user identity of the served user and continue with the rest of the steps;

NOTE 5: If the P-Served-User header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

b) if the request does not contain a P-Served-User header field then

i) determine the served user by taking the identity contained in one of the URI(s) of the P-Asserted-Identity header field. In case the determined served user is a barred public user identity, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, the S-CSCF shall save the public user identity of the served user and continue with the rest of the steps; and

ii) if the P-Asserted-Identity header field contains two URIs and the URI other than the determined served user is not an alias of the determined served user or is barred then act based on local policy, e.g. reject the request by generating a 403 (Forbidden) response or remove the URI not identifying the determined served user from the P-Asserted-Identity header field;

NOTE 6: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

1A) if the Contact is a GRUU, but is not valid as defined in subclause 5.4.7A.4, then return a 4xx response as specified in RFC 5627 [93];

2) store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field if present, and remove it from any forwarded request;

NOTE 7: Any received "orig-ioi" header field parameter will be either a type 1 IOI or a type 3 IOI. The type 1 IOI identifies the network from which the request was sent and the type 3 IOI identifies the service provider from which the request was sent (AS initiating a session on behalf of a user or a PSI);

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header field is present in the topmost Route header field of the incoming request.

- If not present, the S-CSCF shall build an ordered list of initial filter criteria based on the public user identity of the served user (as determined in step 1) of the received request as described in 3GPP TS 23.218 [5].

- If present, the request has been sent from an AS in response to a previously sent request, an ordered list of initial filter criteria already exists and the S-CSCF shall not change the ordered list of initial filter criteria even if the AS has changed the P-Served-User header field or the P-Asserted-Identity header field;

NOTE 8: An original dialog identifier is sent to each AS invoked due to iFC evaluation such that the S-CSCF can associate requests as part of the same sequence that trigger iFC evaluation in priority order (and not rely on SIP dialog information that can change due to B2BUA AS). If the same original dialog identifier is included in more than one request from a particular AS (based on service logic in the AS), then the S-CSCF will continue the iFC evaluation sequence rather than build a new ordered list of iFC;

4) remove its own SIP URI from the topmost Route header field;

4A) if a reference location was received from the HSS at registration as part of the user profile and the request does not contain a message body with the content type application/pidf+xml in accordance with RFC 6442 [89] and does not contain a P-Access-Network-Info header field containing the "network-provided" parameter, the S-CSCF shall insert a P-Access-Network-Info header field constructed according to the reference location received from the HSS and containing the "network-provided" parameter. The access type information received from the HSS shall be mapped into the corresponding access-type parameter of the P-Access-Network-Info header field and the location information shall be mapped into the location parameter corresponding to the access-type parameter, i.e. into "dsl-location" parameter, "fiber-location" parameter or "eth-location" parameter;

4B) if there was an original dialog identifier present in the topmost Route header field of the incoming request and the request is received from a functional entity within the same trust domain and contains a P-Asserted-Service header field, continue the procedure with step 5;

4C) if the request contains a P-Preferred-Service header field, check whether the ICSI value contained in the P-Preferred-Service header field is part of the set of the subscribed services for the served user and determine, using operator-configured data, whether the contents of the request match the ICSI for the subscribed service. The operator-configured data used to determine if there is a matching between the request and the ICSI value may be based on any information in the request (e.g. SDP media capabilities, Content-Type header field, request method). Then:

a) if there is no match between the request and the ICSI value, as an operator option, the S-CSCF may reject the request by generating a 403 (Forbidden) response. Otherwise remove the P-Preferred-Service header field and continue with the rest of the steps; and

b) if there is a match between the request and the ICSI value, then include a P-Asserted-Service header field in the request containing the ICSI value contained in the P-Preferred-Service header field, remove the P-Preferred-Service header field, and continue the procedure with step 5;

4D) if the request does not contain a P-Preferred-Service header field, check, using operator-configured data, whether the contents of the request match a subscribed service for each and any of the subscribed services for the served user:

a) if not, as an operator option, the S-CSCF may reject the request by generating a 403 (Forbidden) response; and

b) if so, and if the request is related to an IMS communication service and the IMS communication service requires the use of an ICSI value then select an ICSI value for the related IMS communication service and include a P-Asserted-Service header field in the request containing the selected ICSI value; and

NOTE 9: If more than one ICSI values match the contents of the request, the S-CSCF selects an ICSI value based on local policy.

c) if so, and if the request is related to an IMS communication service and the IMS communication service does not require the use of an ICSI value then continue without including an ICSI value; and

d) if so, and if the request does not relate to an IMS communication service (or if the S-CSCF is unable to unambiguously determine the service being requested but decides to allow the session to continue) then continue without including an ICSI value;

5) check whether the initial request matches any unexecuted initial filter criteria. If there is a match, then the S-CSCF shall select the first matching unexecuted initial filter criteria from the ordered list of initial filter criteria and the S-CSCF shall:

a) insert the AS URI to be contacted into the Route header field as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 10: If the AS is accessed via an ISC gateway function, then the URI will be the address of the ISC gateway function.

b) if the S-CSCF supports the P-Served-User extension as specified in RFC 5502 [133] and RFC 8498 [239] insert P-Served-User header field populated with the served user identity as determined in step 1. If required by operator policy, the S-CSCF shall:

- if the associated session case is "Originating" as specified in 3GPP TS 29.228 [14], include the sescase header field parameter set to "orig" and the regstate header field parameter set to "reg";

- if the associated session case is "Originating\_Unregistered" as specified in 3GPP TS 29.228 [14], include the sescase header field parameter set to "orig" and the regstate header field parameter set to "unreg";

- if the associated session case is "Originating\_CDIV" as specified in 3GPP TS 29.228 [14], include the "orig-cdiv" header field parameter, defined in RFC 8498 [239]; and

c) if the AS is located outside the trust domain then the S-CSCF shall remove the access-network-charging-info parameter in the P-Charging-Vector header field from the request that is forwarded to the AS; if the AS is located within the trust domain, then the S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field in the request that is forwarded to the AS;

d) insert a type 3 "orig-ioi" header field parameter in place of any received "orig-ioi" header field parameters in the P-Charging-Vector header field. The S-CSCF shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The S-CSCF shall not include the type 3 "term-ioi" header field parameter;

e) remove the "transit-ioi" header field parameter, if received;

f) based on operator policy insert in a Relayed-Charge header field the value of the received "transit-ioi" header field parameter in the P-Charging-Vector header field;

g) based on local policy, the S-CSCF shall add an "fe-addr" element of the "fe-identifier" header field parameter to the P-Charging-Vector header field with its own address or identifier;

h) if the S-CSCF supports using a token to identify the registration and if a registration exists, insert a "+g.3gpp.registration-token" Feature-Caps header field parameter, as defined in subclause 7.9A.8, set to the same value as included in the "+g.3gpp.registration-token" Contact header field parameter of the third party REGISTER request sent to the AS when the UE registered; and

i) if an IP address associated with the served user and the AS SIP URI is stored as described in subclause 5.4.0 exists, then the S-CSCF forwards the SIP message to the IP address associated with the served user and the AS SIP URI;

NOTE 11: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request-URI.

NOTE 12: An AS can activate or deactivate its own filter criteria via the Sh interface. As the S-CSCF checks initial filter criteria only on receipt of an initial request for a dialog, or a standalone transaction, a modified service profile will have no impact on transactions or dialogs already in progress and the modified profile will be effective only for new transactions and dialogs. If the S-CSCF receives a modification of the iFC during their execution, then it should not update the stored initial Filter Criteria until the iFC related to the initial request have been completely executed.

6) if there was no original dialog identifier present in the topmost Route header field of the incoming request store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field. Optionally, the S-CSCF may generate a new, globally unique ICID and insert the new value in the "icid-value" header field parameter of the P-Charging-Vector header field when forwarding the message. If the S-CSCF creates a new ICID, then it is responsible for maintaining the two ICID values in the subsequent messaging. Based on local policy, the S-CSCF shall add an "fe-addr" element of the "fe-identifier" header field parameter to the P-Charging-Vector header field with its own address or identifier if not already available;

7) in step 5, if the initial request did not match any unexecuted initial filter criteria (i.e. the request is not forwarded to an AS):

a) remove the received "transit-ioi" from the P-Charging-Vector header field, if present;

b) insert a type 2 "orig-ioi" header field parameter into the P-Charging-Vector header field. The S-CSCF shall set the type 2 "orig-ioi" header field parameter to a value that identifies the sending network. The S-CSCF shall not include the type 2 "term-ioi" header field parameter; and

c) remove the Relayed-Charge header field, if present;

8) insert a P-Charging-Function-Addresses header field populated with values received from the HSS if the request does not contain a P-Charging-Function-Addresses header field and the message is forwarded within the S-CSCF home network, including towards AS;

9) if there was no original dialog identifier present in the topmost Route header field of the incoming request and if the served user is not considered a privileged sender then:

a) if the P-Asserted-Identity header field contains only a SIP URI and if the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header field is an alias SIP URI for a tel URI, add a second P-Asserted-Identity header field containing this tel-URI, including the display name associated with the tel URI, if available; and

b) if the P-Asserted-Identity header field contains only a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home network domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CSCF shall also add a "user" SIP URI parameter equals "phone" to the SIP URI;

NOTE 13: If tel URI is shared URI so is the alias SIP URI.

10) if the request is not forwarded to an AS and if the outgoing Request-URI is:

- a SIP URI with the user part starting with a + and the "user" SIP URI parameter equals "phone", and if configured per local operator policy, the S-CSCF shall perform the procedure described here. Local policy can dictate whether this procedure is performed for all domains of the SIP URI, only if the domain belongs to the home network, or not at all. If local policy indicates that the procedure is to be performed, then the S-CSCF shall translate the international public telecommunications number contained in the user part of the SIP URI (see RFC 3966 [22]) to a globally routeable SIP URI using either an ENUM/DNS translation mechanism with the format specified in RFC 6116 [24], or any other available database. Database aspects of ENUM are outside the scope of the present document. An S-CSCF that implements the additional routeing functionality described in annex I may forward the request without attempting translation. If an agreement exists between the home network and the visited network to support roaming architecture for voice over IMS with local breakout, the S-CSCF does not enable NP capabilities, and the S-CSCF decides to loopback the call to the visited network, the S-CSCF may forward the request without attempting translation. If a translation is in fact performed and it succeeds, the S-CSCF shall update the Request-URI with the globally routeable SIP URI either returned by ENUM/DNS or obtained from any other available database. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g. a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. When forwarding the request to a BGCF or any other appropriate entity, the S-CSCF shall leave the original Request-URI containing the SIP URI with "user" SIP URI parameter equals phone unmodified. If the request is forwarded, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header field prior to forwarding the message;

- a SIP URI with a "user" SIP URI parameter equals "dialstring" and the domain name of the SIP URI belongs to the home network (i.e. the local number analysis and handling is either failed in the appropriate AS or the request has not been forwarded to AS for local number analysis and handling at all), either forward the request to any appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or send an appropriate SIP response to the originator;

- a SIP URI with a local number (see RFC 3966 [22]) in the user part and a "user" SIP URI parameter equals "phone" and the domain name of the SIP URI belongs to the home network (i.e. the local number analysis and handling is either failed in the appropriate AS or the request has not been forwarded to AS for local number analysis and handling at all), either forward the request to to a BGCFor any appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or send an appropriate SIP response to the originator;

- a tel URI containing a global number (see RFC 3966 [22]) in the international format, the S-CSCF shall translate the E.164 address to a globally routeable SIP URI using either an ENUM/DNS translation mechanism with the format specified in RFC 6116 [24], or any other available database. Database aspects of ENUM are outside the scope of the present document. An S-CSCF that implements the additional routeing functionality described in annex I may forward the request without attempting translation. If an agreement exists between the home network and the visited network to support roaming architecture for voice over IMS with local breakout, the S-CSCF does not enable NP capabilities, and the S-CSCF decides to loopback the call to the visited network, the S-CSCF may forward the request without attempting translation. If this translation is in fact performed and it succeeds, the S-CSCF shall update the Request-URI with the globally routeable SIP URI returned by ENUM/DNS or any other available database. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. When forwarding the request to a BGCF or any other appropriate entity, the S-CSCF shall leave the original Request-URI containing the tel URI unmodified. If the request is forwarded, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header field prior to forwarding the message;

- a tel URI containing a local number (see RFC 3966 [22]) (i.e. the local number analysis and handling is either failed in the appropriate AS or the request has not been forwarded to AS for local number analysis and handling at all), either forward the request to a BGCF or any other appropriate entity (e.g. a MRFC to play an announcement) in the originator's home network or send an appropriate SIP response to the originator;

- a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI: and

- a service URN, e.g. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. In this case the S-CSCF shall not modify the received Request-URI.

NOTE 14: If there is no SIP-based transport found after applying the procedure specified in RFC 3861 [63], the S-CSCF can forward the request to a translating gateway.

Additional procedures apply if the S-CSCF supports NP capabilities and these capabilities are enabled by local policy, and the database used for translation from an international public telecommunications number to a SIP URI also provides NP data (for example, based on the PSTN Enumservice as defined by RFC 4769 [114] or other appropriate data bases). If the above translation from an international public telecommunications number to a SIP URI failed, but NP data was obtained from the database and there is no "npdi" parameter in the received request, then the S-CSCF shall, based on operator policy, replace the URI in the Request-URI with the obtained NP data, prior to forwarding the request to the BGCF or other appropriate entity. If the received request already contains a tel-URI "npdi" parameter, then the S-CSCF may update the URI with the obtained NP data. The URI is updated by the S-CSCF by adding NP parameters defined by RFC 4694 [112]. If the Request-URI is a tel-URI, then an "npdi" tel-URI parameter is added to indicate that NP data retrieval has been performed, and if the number is ported, an "rn" tel-URI parameter is added to identify the ported-to routeing number. If the Request-URI is in the form of a SIP URI user=phone, the "npdi" and "rn" tel-URI parameters are added as described above to the userinfo part of the SIP URI;

NOTE 15: When the S-CSCF replaces the tel-URI in the Request-URI with the obtained NP data, all tel URI parameters in the received Request-URI will be replaced by the obtained NP data.

10A) if the request is not forwarded to an AS and if local policy requires the application of additional routeing capabilities, as defined in annex I, the S-CSCF shall apply the additional routeing capabilities if they are locally available or forward the request to an entity that implements the additional routeing capabilities;

10B) if an agreement exists between the home network and the visited network to support Roaming Architecture for Voice over IMS with Local Breakout then continue with the following steps. Otherwise continue with step 11. If:

- the top most Route header contains an indication that this is the UE-originating case;

NOTE 16: This indication can e.g. be in a URI parameter, a character string in the user part of the URI or can be a port number in the URI added by the S-CSCF during the registration in the Service-Route header field.

- the UE is roaming (as identified by the P-Visited-Network-ID header field value in the original REGISTER request); and

- the request is an INVITE request;

determine if loopback routeing is applicable for this request using local policy, and save this decision for subsequent processing along with the following information:

a) any URI representing the TRF address preference received from the visited network; and

b) the ICID received in the request.

In addition, the S-CSCF shall also include in the request a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter according to RFC 6809 [190] with the "+g.3gpp.home-visited" header field parameter set to the identifier of the visited network received in the P-Visited-Network-ID header field in the original registration request;

10C) if the request is an INVITE request, then determine whether loopback is applied for this request. The information saved in step 10B, and the presence or absence of the Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter in the received INVITE request are taken into account in making this decision:

a) if loopback routeing is not to be performed for this request remove any "+g.3gpp.trf" header field parameter or "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field of the outgoing request;

b) if loopback routeing is applied for this request;

i) remove all entries in the Route header field;

ii) if a "+g.3gpp.trf" header field parameter with a parameter value containing a valid URI, is included in the Feature-Caps header field of the request, insert the URI in a Route header field;

iii) if a "+g.3gpp.trf" header field parameter, with a parameter value containing a valid URI is not included in the Feature-Caps header field of the request, insert a locally configured TRF address, associated with the visited network for this call, in the Route header field;

iv) remove any "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field of the outgoing request;

v) insert the "+g.3gpp.loopback" header field parameter as specified in subclause 7.9A.4 in the Feature-Caps header field of the request, in accordance with the RFC 6809 [190]. If providing the identifier of the home network is supported by the S-CSCF and the visited network, the S‑CSCF may based on operator agreement insert the "+g.3gpp.loopback" header field parameter set to the identifier of the home network;

vi) if included in the incoming request, remove the "+g.3gpp.trf" header field parameter from the Feature-Caps header field from the outgoing request;

vii) remove a type 2 "orig-ioi" header field parameter that was added in step 7 from the P-Charging-Vector header field and insert a type 1 "orig-ioi" header field parameter into the P-Charging-Vector header field. The S-CSCF shall set the type 1 "orig-ioi" header field parameter to a value that identifies the network in which the S-CSCF resides. The S-CSCF shall not include the "term-ioi" header field parameter; and

viii) if the S-CSCF supports indicating the traffic leg associated with a URI as specified in RFC 7549 [225] and if an "iotl" SIP URI parameter is not included in the TRF URI in the Route header field and if required by local policy, append an "iotl" URI parameter with a value set to "homeA-visitedA" to the URI in the Route header field; and

c) if the final decision on loopback routeing is deferred to a subsequent entity in the home network, the BGCF, then the S-CSCF includes, if absent, in the request a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter, with the parameter value set to the identifier of the visited network received in the P-Visited-Network-ID header field in the original registration request. The S-CSCF is expected to know by means of network configuration that such a subsequent entity exists; and

NOTE 17: The subsequent entity in the home network, the BGCF, will remove the "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field when a final routeing decision is taken.

11) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header field if present, otherwise based on the Request-URI. If the destination requires interconnect functionalities (e.g. the destination address is of an IP address type other than the IP address type used in the IM CN subsystem), the S-CSCF shall forward the request to the destination address via an IBCF in the same network;

12) if network hiding is needed due to local policy, put the address of the IBCF to the topmost Route header field;

13) in case of an initial request for a dialog:

a) determine the need for GRUU processing. GRUU processing is required if:

- an original dialog identifier that the S-CSCF previously placed in a Route header field is not present in the topmost Route header field of the incoming request (this means the request is not returning after having been sent to an AS), and

- the contact address contains a GRUU that was either assigned by the S-CSCF that is valid as specified in subclause 5.4.7A.4 or a temporary GRUU self assigned by the UE based on the "temp-gruu-cookie" header parameter provided to the UE;

NOTE 18: The procedures for determining that a URI is a temporary GRUU assigned by the UE are specified in subclause 7.1.2.3 of RFC 6140 [191].

b) if GRUU processing is not required and the initial request originated from a served user, then determine the need to record-route for other reasons:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF shall decide, based on operator policy, whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header field containing its own SIP URI;

- if the request is a SUBSCRIBE request and routed elsewhere, the S-CSCF shall decide, based on operator policy, whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request (e.g. event package name). If the request is record-routed the S-CSCF shall create a Record-Route header field containing its own SIP URI; or

NOTE 19: Some subscriptions to event packages (e.g. presence) can result in virtually persistent subscriptions and if the S-CSCF Record-Routes this can prevent reassignment of the S-CSCF.

NOTE 20: If the S-CSCF does not Record-Route the initial SUBSCRIBE request, it will not be possible to perform SIP digest authentication of SIP requests sent inside the SIP dialog related to the associated subscription.

- if the request not a SUBSCRIBE request and is routed elsewhere, create a Record-Route header field containing its own SIP URI;

NOTE 21: For requests originated from a PSI the S-CSCF can decide whether to record-route or not based on operator policy.

c) if GRUU processing is required, the S-CSCF shall create a Record-Route header field containing its own SIP URI;

d) if GRUU processing is required, the S-CSCF shall save an indication that GRUU-routeing is to be performed for in-dialog requests that reach the S-CSCF because of the Record-route header field added in step c);

NOTE 22: The manner of representing the GRUU-routeing indication is a private matter for the S-CSCF. The indication is used during termination processing of in-dialog requests to cause the S-CSCF to replace a Request-URI containing a GRUU with the corresponding registered contact address. It can be saved using values in the Record-Route header field, or in dialog state.

14) based on the destination user (Request-URI), remove any P-Access-Network-Info header field and the access-network-charging-info parameter in the P-Charging-Vector header field prior to forwarding the message;

14A) if the request is not routed to an AS, to a BGCF or to an entity that implements the additional routeing functionality, remove the P-Served-User header field prior to forwarding the request;

14B) if the S-CSCF supports indicating the traffic leg as specified in RFC 7549 [225], the request is not routed to an AS, to a BGCF or to an entity that implements the additional routeing functionality, loopback routeing is not to be performed for this request, required by local policy and the Request-URI contains a SIP URI, append the "iotl" SIP URI parameter set to "homeA-homeB" to the Request-URI;

15) route the request based on SIP routeing procedures;

16) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

17) if the request contains a "logme"parameter in the Session-ID header field, treat this dialog as one for which logging is in progress and log SIP signalling for this dialog according to its trace configuration;

18) if the S-CSCF supports using a token to identify the registration and if the request is not forwarded to an AS, remove the "+g.3gpp.registration-token" Feature-Caps header field parameter, defined in subclause 7.9A.8, if received in the request; and

19) if the received request is an INVITE request or a MESSAGE request and the S-CSCF supports calling number verification using signature verification and attestation information as specified in subclause 3.1, the S-CSCF shall based on local policy perform attestation of the user identity by inserting:

- a "verstat" tel URI parameter, specified in subclause 7.2A.20, to the tel URI or SIP URI with a user=phone parameter in the From header field or the P-Asserted-Identity header field;

an Origination-Id header field, specified in subclause 7.2.19, set to a UUID identifying the S-CSCF which is configured based on local policy and requirements from national regulation: and

- an Attestation-Info header field, specified in subclause 7.2.18, set to the value "A".

When the S-CSCF receives, an initial request for a dialog or a request for a standalone transaction, from an AS acting on behalf of an unregistered user, the S-CSCF shall:

1) execute the procedures described in the steps 1, 2, 3, 4, 4B, 4C, 4D, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 and 16 in the above paragraph (when the S-CSCF receives, from a registered served user, an initial request for a dialog or a request for a standalone transaction).

NOTE 23: When the S-CSCF does not have the user profile, before executing the actions as listed above, it initiates the S-CSCF Registration/deregistration notification procedure, as described in 3GPP TS 29.228 [14]; with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informs the HSS that the user is unregistered. The S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14]. When requesting the user profile, and the request received by the S-CSCF contains a P-Profile-Key header field, the S-CSCF can include the header field value in S-CSCF Registration/deregistration notification. If the response from the HSS includes a Wildcarded Public Identity AVP, and if the request received by the S-CSCF did not include a P-Profile-Key header field, the S-CSCF uses the AVP value to set the P-Profile-Key header field before forwarding the request to an AS.

When the S-CSCF receives a request initiated by the served user for which the S-CSCF does not have the user profile or does not trust the data that it has (e.g. due to restart), the S-CSCF shall attempt to retrieve the user profile from the HSS. If the S-CSCF receives a Diameter result code of DIAMETER\_UNABLE\_TO\_COMPLY as defined in 3GPP TS 29.228 [14], the S-CSCF supports S-CSCF restoration procedures, and the Request-URI of the request does not match an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], then the S-CSCF shall:

I) reject the request by returning a 504 (Server Time-out) response to the UE;

II) assume that the UE supports version 1 of the XML Schema for the 3GPP IM CN subsystem XML body if support for the 3GPP IM CN subsystem XML body as described in subclause 7.6 in the Accept header field is not indicated; and

III) include in the 504 (Server Time-out) response:

- a Content-Type header field with the value set to associated MIME type of the 3GPP IM CN subsystem XML body as described in subclause 7.6.1;

- a P-Asserted-Identity header field set to the value of the SIP URI of the S-CSCF included in the Service-Route header field (see subclause 5.4.1.2.2F) during the registration of the user whose UE sent the request causing this response; and

- a 3GPP IM CN subsystem XML body:

a) an <ims-3gpp> element with the "version" attribute set to "1" and with an <alternative-service> child element, set to the parameters of the alternative service;

i) a <type> child element, set to "restoration" (see table 7.6.2) to indicate that S-CSCF restoration procedures are supported;

ii) a <reason> child element, set to an operator configurable reason; and

iii) an <action> child element, set to "initial-registration" (see table 7.6.3).

NOTE 24: These procedures do not prevent the usage of unspecified reliability or recovery techniques above and beyond those specified in this subclause.

Depending on operator configuration (see subclause 5.4.1.8), when the S-CSCF receives a request with a Request-URI that does not match an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], the request initiated by the served user for which the S-CSCF has modified but not synchronized the service profile for the served user and the S-CSCF supports S-CSCF restoration procedures, then the S-CSCF shall reject the request as described in items I), II) and III).

If the S-CSCF:

a) fails to receive a SIP response within a configurable time; or

b) receives a 408 (Request Timeout) response or a 5xx response from the AS without previously receiving a 1xx response to the original SIP request, and without previously receiving a SIP request from the AS that contained the same original dialog identifier as the original request;

the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION\_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 5; and

- if the default handling defined in the filter criteria indicates the value "SESSION\_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or, if the request is an initial INVITE request, send a 408 (Request Timeout) response or a 5xx response towards the served UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, the S-CSCF shall forward the response towards the served UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives any response to the above request containing a Relayed-Charge header field, and the next hop is not an AS, the S-CSCF shall remove the Relayed-Charge header field from the forwarded response.

When the S-CSCF receives any response to the above request, the S-CSCF may:

1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header field.

NOTE 25: The P-Asserted-Identity header field would normally only be expected in 1xx or 2xx responses.

NOTE 26: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

When the S-CSCF receives any response to the above request, the S-CSCF shall:

1) If logging is in progress for this dialog, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred then stop treating this as a dialog for which logging is in progress, else the S-CSCF shall append a "logme" header field parameter to the SIP Session-ID header field if the parameter is missing and determine, by checking its trace configuration, whether to log the response.

When the S-CSCF receives any response to the above request containing a "term-ioi" header field parameter in the P-Charging-Vector header field, the S-CSCF shall:

1) store the value of the received "term-ioi" header field parameter if present;

2) remove all received "orig-ioi", "term-ioi" and "transit-ioi" header field parameters from the forwarded response;

3) include the stored "orig-ioi" header field parameter if received in the request;

4) include a type 1 "term-ioi" header field parameter if next hop is not an AS, or a type 3 "term-ioi" header field parameter. The "term-ioi" header field parameter is set to a value that identifies the sending network of the response

NOTE 27: Any received "term-ioi" header field parameter will be a type 2 IOI, if received from an S-CSCF, or type 3 IOI, if received from an AS, or type 1 IOI if the S-CSCF performed loopback routeing for this request. A type 2 IOI identifies the sending network of the response, a type 3 IOI identifies the sending service provider of the response, and a type 1 IOI identifies the visited network of the served user.

5) based on operator policy include any received "transit-ioi" header field parameter, from the P-Charging-Vector header field, in a Relayed-Charge header field, if the next hop is an AS.

When the S-CSCF receives any 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

When the S-CSCF receives any 1xx or 2xx response to an initial request for a dialog or a request for a standalone transaction, if the response is forwarded within the S-CSCF home network and not to an AS, the S-CSCF shall insert a P-Charging-Function-Addresses header field populated with values received from the HSS.

When the S-CSCF, upon sending an initial INVITE request that includes an IP address in the SDP offer (in "c=" parameter), receives an error response indicating that the IP address type is not supported, (e.g., the S-CSCF receives the 488 (Not Acceptable Here) with 301 Warning header field indicating "incompatible network address format"), the S-CSCF shall either:

- fork the initial INVITE request to the IBCF; or

- process the error response and forward it using the Via header field.

NOTE 28: If the S-CSCF knows that the originating UE supports both IPv6 and IPv4 addresses simultaneously, the S-CSCF will forward the error response to the UE using the Via header field. The present version of the specification does not specify how the S-CSCF determines whether the UE supports both IPv6 and IPv4 addressing simultaneously.

When the S-CSCF receives from the served user a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

0A) if the dialog is related to an IMS communication service determine whether the contents of the request (e.g. SDP media capabilities, Content-Type header field) match the IMS communication service as received as the ICSI value in the P-Asserted-Service header field in the initial request. As an operator option, if the contents of the request do not match the IMS communication service the S-CSCF may reject the request by generating a status code reflecting which added contents are not matching. Otherwise, continue with the rest of the steps;

1) remove its own URI from the topmost Route header field;

2) create a Record-Route header field containing its own SIP URI;

3) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), save the Contact and CSeq header field values received in the request such that the S-CSCF is able to release the session if needed;

4) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the access-network-charging-info parameter in the P-Charging-Vector header field;

5) route the request based on the topmost Route header field; and

6) if the request was sent on a dialog for which logging of signalling is in progress, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred then stop logging of signalling, else determine, by checking its trace configuration, whether to log the response.

When the S-CSCF receives any response to the above request, the S-CSCF shall:

1) If logging is in progress for this dialog, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred then stop logging of signalling, else determine, by checking its trace configuration, whether to log the response.

When the S-CSCF receives any 1xx or 2xx response to the target refresh request for an INVITE dialog, the S-CSCF shall replace the saved Contact header field values in the response such that the S-CSCF is able to release the session if needed.

If the S-CSCF inserted in the initial request for the dialog the header field parameters into the Feature-Caps header field then the S-CSCF shall include the header field parameters with the same parameter values into the Feature-Caps header field in any target refresh request for the dialog, and in each 1xx or 2xx response to target refresh request sent in the same direction.

When the S-CSCF receives from the served user a subsequent request other than a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

1) remove its own URI from the topmost Route header field;

2) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the access-network-charging-info parameter in the P-Charging-Vector header field; and

3) route the request based on the topmost Route header field; and

4) if the request was sent on a dialog for which logging of signalling is in progress, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred, stop logging of signalling, else determine, by checking its trace configuration, whether to log the request.

When the S-CSCF receives any response to the above request, the S-CSCF shall:

1) If logging is in progress for this dialog, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred then stop logging of signalling, else determine, by checking its trace configuration, whether to log the response.

With the exception of 305 (Use Proxy) responses, the S-CSCF shall not recurse on 3xx responses.

\*\*\*\*\* Fourth change \*\*\*\*\*

#### 5.4.3.3 Requests terminated at the served user

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the S-CSCF shall give priority over other transactions or dialogs. This allows special treatment for such transactions or dialogs. If priority is supported, the S-CSCF shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE 1: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the S-CSCF receives, destined for a registered served user, an initial request for a dialog or a request for a standalone transaction, and the request is received either from a functional entity within the same trust domain or contains a valid original dialog identifier or the dialog identifier (From, To and Call-ID header fields) relates to an existing request processed by the S-CSCF, then prior to forwarding the request, the S-CSCF shall:

1) check if an original dialog identifier that the S-CSCF previously placed in a Route header field is present in the topmost Route header field of the incoming request.

- If present, the request has been sent from an AS in response to a previously sent request.

- If not present, it indicates that the request is visiting the S-CSCF for the first time and in this case the S-CSCF shall determine the served user by taking the identity contained in the Request-URI. If the Request-URI is a temporary GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.3, then take the public user identity that is associated with the temporary GRUU to be the served user identity. Then check whether the determined served user identity is a barred public user identity. In case the served user identity is a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 404 (Not Found) response. Otherwise, the S-CSCF shall save the Request-URI from the request, the served user identity and the public user identity of the served user and continue with the rest of the steps;

NOTE 2: An original dialog identifier is sent to each AS invoked due to iFC evaluation such that the S-CSCF can associate requests as part of the same sequence that trigger iFC evaluation in priority order (and not rely on SIP dialog information that can change due to B2BUA AS). If the same original dialog identifier is included in more than one request from a particular AS (based on service logic in the AS), then the S-CSCF will continue the iFC evaluation sequence rather than build a new ordered list of iFC;

2) remove its own URI from the topmost Route header field;

2A) if there was no original dialog identifier present in the topmost Route header field of the incoming request build an ordered list of initial filter criteria based on the public user identity in the Request-URI of the received request as described in 3GPP TS 23.218 [5].

3) if there was an original dialog identifier present in the topmost Route header field of the incoming request then check whether the Request-URI matches the saved Request-URI. The Request-URI and saved Request-URI are considered a match:

a) if the canonical forms of the two Request-URI are equal to the saved value of the Request-URI;

b) if the Request-URI is a GRUU (public or temporary) and the saved value of the Request-URI is a GRUU (public or temporary) and both GRUUs represent the same public user identity or represent public user identities that are alias SIP URIs of each other; or

c) if the Request-URI is an alias SIP URI of the saved value of the Request-URI.

NOTE 3: The canonical form of the Request-URI is obtained by removing all URI parameters (including the user-param), and by converting any escaped characters into unescaped form. The alias SIP URI is defined in subclause 3.1.

If there is no match, then the S-CSCF shall decide whether to trigger the originating services to be executed after retargeting. The decision is configured in the S-CSCF and may use any information in the received request that is used for the initial filter criteria or an operator policy. The S-CSCF shall decide either to:

a) stop evaluating current iFC. In that case, if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed, forward the request based on the topmost Route header field or if not available forward the request based on the Request-URI (routeing based on Request-URI is specified in steps 2, 7 and 10 through 14a from subclause 5.4.3.2) and skip the following steps; or

b) stop evaluating current iFC and build an ordered list of iFC with the originating services to be executed after retargeting as described in 3GPP TS 23.218 [5] criteria based on the public user identity of the served user and start the evaluation of that iFC as described in subclause 5.4.3.2 starting at step 4B of subclause 5.4.3.2;

NOTE 4: The S-CSCF assesses triggering of services for the originating services after retargeting means it evaluates IFCs with a SessionCase set to ORIGINATING\_CDIV, as defined in 3GPP TS 29.228 [14]. If the P-Served-User extension specified in RFC 5502 [133] is supported, the S-CSCF uses the "orig-cdiv" header field parameter defined in RFC 8498 [239].

NOTE 5: The identity of the served user can be obtained from the History-Info header field (see RFC 7044 [66]) or the P-Served User header field as specified in RFC 5502 [133]. The served user can be a public user identity, a public GRUU, or a temporary GRUU. It needs to be ensure, that all ASs in the iFC can determine the served user correctly.

NOTE 6: The S-CSCF determines whether to apply a) or b) based on information in the initial Filter Criteria.

3A) if the Request-URI is a GRUU, but is not valid as defined in subclause 5.4.7A.4, then return a 4xx response as specified in RFC 5627 [93];

3B) if the Request-URI contains a public GRUU and the saved value of the Request-URI is a temporary GRUU, then replace the Request-URI with the saved value of the Request-URI;

3C) if the request contains a P-Asserted-Service header field check whether the IMS communication service identified by the ICSI value contained in the P-Asserted-Service header field is allowed by the subscribed services for the served user:

a) if so, continue from step 4; and

b) if not, as an operator option, the S-CSCF may reject the request by generating a 403 (Forbidden) response. Otherwise, remove the P-Asserted-Service header field and continue with the rest of the steps;

3D) if the request does not contain a P-Asserted-Service header field check if the contents of the request matches a subscribed service (e.g. SDP media capabilities, Content-Type header field) for each and any of the subscribed services for the served user:

a) if not, as an operator option, the S-CSCF may reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps; and

b) if so, and if the request is related to an IMS communication service and the IMS communication service requires the use of an ICSI value then include a P-Asserted-Service header field in the request containing the ICSI value for the related IMS communication service, and use it as a header field in the initial request when matching initial filter criteria in step 4; and

c) if so, and if the request is related to an IMS communication service and the IMS communication service does not require the use of an ICSI value then continue without including an ICSI value; and

d) if so, and if the request does not relate to an IMS communication service (or if the S-CSCF is unable to unambiguously determine the service being requested but decides to allow the session to continue) then continue without inclding an ICSI value;

4) check whether the initial request matches any unexecuted initial filter criteria based on the public user identity of the served user in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then the S-CSCF shall select the first matching unexecuted initial filter criteria and:

a) if the Request-URI is a temporary GRUU as defined in subclause 5.4.7A.3, then replace the Request-URI with the public GRUU that is associated with the temporary GRUU (i.e. the public GRUU representing the same public user identity and instance ID as the temporary GRUU);

b) insert the AS URI to be contacted into the Route header field as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

c) if the S-CSCF supports the P-Served-User extension as specified in RFC 5502 [133], insert the P-Served-User header field populated with the served user identity as determined in step 1. If required by operator policy, the S-CSCF shall:

- if the associated session case is "Terminating" as specified in 3GPP TS 29.228 [14], include the sescase header field parameter set to "term" and the regstate header field parameter set to "reg";

- if the associated session case is "Terminating\_Unregistered" as specified in 3GPP TS 29.228 [14], include the sescase header field parameter set to "term" and the regstate header field parameter set to "unreg";

d) insert a type 3 "orig-ioi" header field parameter replacing any received "orig-ioi" header field parameter in the P-Charging-Vector header field. The type 3 "orig-ioi" header field parameter identifies the sending network of the request message. The S-CSCF shall not include the type 3 "term-ioi" header field parameter;

e) based on local policy, the S-CSCF shall add an "fe-addr" element of the "fe-identifier" header field parameter to the P-Charging-Vector header field with its own address or identifier if not already available;

f) remove the "transit-ioi" header field parameter, if received;

g) based on operator policy insert a Relayed-Charge header field containing the value of the received "transit-ioi" header field parameter in the P-Charging-Vector header field; and

h) if an IP address associated with the served user and the AS SIP URI is stored as described in subclause 5.4.0 exists, then the S-CSCF forwards the SIP message to the IP address associated with the served user and the AS SIP URI;

NOTE 7: Depending on the result of the previous process, the S-CSCF can contact one or more AS(s) before processing the outgoing Request-URI.

NOTE 8: If the Request-URI of the received terminating request contains a temporary GRUU, then step 4 replaces the Request-URI with the associated public GRUU before invoking the AS, and step 3B restores the original temporary GRUU when the request is returned from the AS.

NOTE 9: An AS can activate or deactivate its own filter criteria via the Sh interface. As the S-CSCF checks initial filter criteria only on receipt of an initial request for a dialog, or a standalone transaction, a modified service profile will have no impact on transactions or dialogs already in progress and the modified profile will be effective only for new transactions and dialogs. If the S-CSCF receives a modification of the iFC during their execution, then it should not update the stored initial Filter Criteria until the iFC related to the initial request have been completely executed.

5) if there was no original dialog identifier present in the topmost Route header field of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

6) if there was no original dialog identifier present in the topmost Route header field of the incoming request store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field;

7) if there was no original dialog identifier present in the topmost Route header field of the incoming request:

- store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field, if present;

- remove received "orig-ioi", "term-ioi" and "transit-ioi" header field parameters from the forwarded request if next hop is not an AS; and

- include a type 1 "orig-ioi" header field parameter if next hop is not an AS;

NOTE 10: Any received "orig-ioi" header field parameter will be a type 2 IOI. or type 3 IOI. A type 2 IOI identifies the sending network of the request message, a type 3 IOI identifies the sending service provider of the request message.

7A) if there was an original dialog identifier present in the topmost Route header field of the incoming request:

- store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field, if present;

- remove the received "orig-ioi" header field parameter if next hop is not an AS;

- include a type 1 "orig-ioi" header field parameter if next hop is not an AS;

- based on local policy, the S-CSCF shall add an "fe-addr" element of the "fe-identifier" header field parameter to the P-Charging-Vector header field with its own address or if not already available; and

- remove any received Relayed-Charge header field if next hop is not an AS;

NOTE 11: Any received "orig-ioi" header field parameter will be a type 3 IOI. A type 3 IOI identifies the sending service provider of the request message.

8) in the case:

i) there are no Route header fields in the request; and

ii) there are bindings saved during registration or re-registration as described in subclause 5.4.1.2 which are not marked as created by an emergency registration as described in subclause 5.4.8.2;

then, create a target set of potential routes from the list of preloaded routes associated with the bindings in item 8) ii), as follows:

a) if the Request-URI contains a valid GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that does not contain a "bnc" URI parameter, then the target set is determined by following the procedures for Request Targeting specified in RFC 5627 [93], using the public user identity and instance ID derived from the GRUU using the procedures of subclause 5.4.7A;

b) if the Request-URI contains a valid public GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that contains a "bnc" URI parameter then the target set is determined by following the procedures for routeing of public GRUUs specified in RFC 6140 [191].

NOTE 12: The procedures for Request Targeting for public GRUUs in subclause 7.1.1 of RFC 6140 [191] involve copying the "sg" SIP URI parameter from the Public GRUU into the Request-URI along with the bound registered Contact Address.

NOTE 13: In this release of the specification, use of preloaded routes saved during registration or re-registration which created or refreshed bindings marked as created by an emergency registration is out of scope.

c) if the Request-URI contains a temporary GRUU not assigned by the S-CSCF but that contains "temp-gruu-cookie" information provided by the S-CSCF to the UE in a "temp-gruu-cookie" header field parameter as specified in RFC 6140 [191] then the target set is determined by following the procedures for Request Targeting for temporary GRUUs specified in RFC 6140 [191]; or

NOTE 14: The procedures for obtaining the "temp-gruu-cookie" information from the temporary GRUU and for routeing of temporary GRUUs are specified in subclause 7.1.2.3 of RFC 6140 [191].

d) if the Request-URI contains a public user identity or a GRUU not assigned by the S-CSCF, then the target set is all the registered contacts saved for the destination public user identity;

9) if necessary perform the caller preferences to callee capabilities matching according to RFC 3841 [56B] to the target set;

NOTE 15: This might eliminate entries and reorder the target set.

NOTE 16: The S-CSCF performs caller preferences to callee capabilities matching also to select among multiple targets set to a single instance-id, when the UE has registered multiple registration flows.

10) in case there are no Route header fields in the request:

a) if there is more than one route in the target set determined in steps 8) and 9) above:

- if the fork directive in the Request-Disposition header field was set to "no-fork", use the contact with the highest qvalue parameter to build the target URI. In case no qvalue parameters were provided, the S-CSCF shall decide locally what contact address to be used to build the target URI;

- if the fork directive in the Request-Disposition header field was not set to "no-fork", fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header field in the REGISTER request, as described in RFC 3261 [26]. In case no qvalue parameters were provided, then the S-CSCF determine the contact address to be used to build the target URI as directed by the Request-Disposition header field as described in RFC 3841 [56B]. If the Request-Disposition header field is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;

- in case that no route is chosen, return a 480 (Temporarily unavailable) response or another appropriate unsuccessful SIP response and terminate these procedures; and

- per the rules defined in RFC 5626 [92], the S-SCSF shall not populate the target set with more than one contact with the same public user identity and instance-id at a time. If a request for a particular public user identity and instance-id fails with a 430 response, the S-CSCF shall replace the failed branch with another target with the same public user identity and instance-id, but a different reg-id;

b) If no "Loose-Route Indication" indicating the HSS requires the loose-route mechanism as described in 3GPP TS 29.228 [14] has been received, in the service profile of the served public user identity, from the HSS during registration, build the Request-URI with the contents of the target URI determined in the previous step, otherwise the Request-URI is retained as received;

c) insert a P-Called-Party-ID SIP header field containing the contents of the Request-URI (if no "Loose-Route Indication" indicating the HSS requires the loose-route mechanism as described in 3GPP TS 29.228 [14] has been received, in the service profile of the served public user identity, from the HSS during registration, then exclude "rn" tel-URI parameter and "npdi" tel-URI parameter as defined in RFC 4694 [112]) received in the request unless the Request-URI contains a temporary GRUU in which case insert the public GRUU in the P-Called-Party-ID;

d) build the Route header field with the Path values from the chosen route and if "Loose-Route Indication" indicating the HSS requires the loose-route mechanism as described in 3GPP TS 29.228 [14] has been received, in the service profile of the served user identity, from the HSS during registration and the selected contact address was not registered as described in RFC 5626 [92], add the content of the target URI determined in step a), as last URI of the route. If the selected contact address was registered as described in RFC 5626 [92], the target URI determined in step a) is not added to the Route header field; and

e) save the Request-URI and the total number of Record-Route header fields as part of the dialog request state.

NOTE 17: For each initial dialog request terminated at a served user two pieces of state are maintained to assist in processing GRUUs: the chosen contact address to which the request is routed; and the position of an entry for the S-CSCF in the Record-Route header field that will be responsible for GRUU translation, if needed (the position is the number of entries in the list before the entry was added). The entry will be added in step 5) of the below procedures for handling S-CSCF receipt any 1xx or 2xx response to the initial request for a dialog. The S-CSCF can record-route multiple times, but only one of those (the last) will be responsible for gruu translation at the terminating end.

11) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

12) optionally, apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header field and privacy required by RFC 7044 [66]. The S-CSCF shall not remove any priv-value from the Privacy header field;

NOTE 18: keeping the priv-value in the Privacy header field is necessary to indicate to the UE that the public user identity was not sent because of restriction. Although RFC 3323 [33] states that when a privacy service performs one of the functions corresponding to a privacy level listed in the Privacy header field, it SHOULD remove the corresponding priv-value from the Privacy header field, there is no harm that the S-CSCF does not remove the priv-values as there will be no other entity that would perform the privacy service after the S-CSCF.

NOTE 19: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

13) in case of an initial request for a dialog, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF shall decide, based on operator policy, whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header field containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header field containing its own SIP URI;

13A) if the request is routed towards the UE remove the P-User-Database header field and P-Served-User header field if present;

13B) void

13C) if the request was sent on a dialog for which logging of signalling is in progress, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred, stop treating the dialog as one for which logging of signalling is in progress, else append a "logme" header field parameter to the SIP Session-ID header field if the parameter is missing and determine, by checking its trace configuration, whether to log the request;

13D) if the request is routed towards the UE,

- the S-CSCF supports indicating the traffic leg as specified in RFC 7549 [225];

- the UE is roaming; and

- required by local policy;

then:

- if the bottommost Route header field does not contain the "tokenized-by" header field parameter and an "iotl" SIP URI parameter is not already included, append an "iotl" SIP URI parameter set to "homeB-visitedB" to the URI of the bottommost Route header field; and

- if the bottommost Route header field contains the "tokenized-by" header field parameter and an "iotl" SIP URI parameter is not already included, append an "iotl" SIP URI parameter set to "homeB-visitedB" to the URI of the second Route header field from the bottom;

NOTE 20: The bottommost Route header field contains an "iotl" SIP URI parameter if the P‑CSCF added the "iotl" SIP URI parameter in the Path header field during registration and if the visited network does not apply topology hiding. The second Route header field from the bottom contains an "iotl" SIP URI parameter if the P‑CSCF added the "iotl" SIP URI parameter in the Path header field during registration and if the visited network applied topology hiding.

13E) if the S-CSCF supports HSS based P-CSCF restoration and the S-CSCF considers the P-CSCF, identified by the bottommost Route header field, is not reachable:

- reject the request with a 480 (Temporarily Unavailable) response; and

- initiate the HSS based P-CSCF restoration procedure towards the served user as specified in 3GPP TS 23.380 [7D];

13F) if the S-CSCF supports PCRF based P-CSCF restoration procedures, insert a Restoration-Info header field including the IMSI value contained in the user profile of the registered served user as a quoted string defined in 3GPP TS 29.228 [14];

NOTE 21: If PCRF based P-CSCF restoration procedure is operated between the home network and the visited network, the operator policy depends on an agreement with the visited network operator.

13G) if the S-CSCF supports PCRF based P-CSCF restoration procedures,

- the request contains a topmost Route header field pointing to a P-CSCF, and

- the S-CSCF considers the P-CSCF is in a non-working state,

remove all entries in the Route header field and add a Route header field set to the URI associated with an alternative P-CSCF; and

NOTE 22: How the SIP URI of the alternative P-CSCF is obtained by the S-CSCF is implementation dependent. The S-CSCF can make sure that selected P-CSCF support the PCRF based P-CSCF restoration procedures based on local configuration.

NOTE 23: It is implementation dependent as to how the S-CSCF determines the P-CSCF is in non-working state.

14) forward the request based on the topmost Route header field.

If the S-CSCF receives any response to the above request, the S-CSCF shall:

1) If the response contains a "logme" header field parameter in the SIP Session-ID header field then log the response based on local policy.

If the S-CSCF supports HSS based P-CSCF restoration and

a) receives a 404 (Not Found) response;

b) fails to receive any SIP response from a P-CSCF serving a non-roaming user within a configurable time; or

NOTE 24: The configurable time needs to be less than timer B and timer F.

c) receives a 408 (Request Timeout) response or a 504 (Server Time-out) response:

- including a Restoration-Info header field defined in subclause 7.2.11 set to "noresponse"; and

- the "+g.3gpp.ics" Contact header field parameter with a value set to "server" was not included in the REGISTER request when the UE registered;

NOTE 25: If this Contact header field parameter is not included the S-CSCF can deduce that the P-CSCF did not respond to the request.

the S-CSCF shall:

- send a 480 (Temporarily Unavailable) response;

- initiate the HSS based P-CSCF restoration procedure towards the served user as specified in 3GPP TS 23.380 [7D]; and

- if b) or c) above applied consider the P-CSCF as not reachable.

If the S-CSCF supports PCRF based P-CSCF restoration and receives a 404 (Not Found) response, the S-CSCF shall consider the P-CSCF to be in a non-working state and shall initiate the PCRF based P-CSCF restoration procedure towards the served user as specified in 3GPP TS 23.380 [7D].

If the S-CSCF:

a) fails to receive a SIP response within a configurable time; or

b) receives a 408 (Request Timeout) response or a 5xx response from the AS without previously receiving a 1xx response to the original SIP request, and without previously receiving a SIP request from the AS that contained the same original dialog identifier as the original request;

the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION\_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and

- if the default handling defined in the filter criteria indicates the value "SESSION\_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or, if the request is an initial INVITE request, send a 408 (Request Timeout) response or a 5xx response towards the originating UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, the S-CSCF shall forward the response towards the originating UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives any response to the above request and forwards it to an AS, the S-CSCF shall remove any "orig-ioi", "term-ioi" and "transit-ioi" header field parameter if received in a P-Charging-Vector header field, insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the request, a type 3 "term-ioi" header field parameter, and based on operator option insert a Relayed-Charge header field in the response. The S-CSCF shall set the type 3 "term-ioi" header field parameter to a value that identifies the sending network of the response, the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter and include in the Relayed-Charge header field the received "transit-ioi" header field parameter from the P-Charging-Vector header field.

NOTE 26: Any received "term-ioi" header field parameter will be a type 1 IOI or a type 3 IOI. The type 1 IOI identifies the network from which the response was sent and the type 3 IOI identifies the service provider from which the response was sent.

When the S-CSCF receives, destined for an unregistered served user or a statically pre-configured PSI, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

1) Void.

2) execute the procedures described in 1, 2, 3, 3C, 3D, 4, 5, 6, 7, 11, 13, 13B, 13C and 14 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

3) In case that no more AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures.

NOTE 27: When the S-CSCF does not have the user profile, before executing the actions as listed above, it initiates the S-CSCF Registration/deregistration notification procedure, as described in 3GPP TS 29.228 [14]; with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informs the HSS that the user is unregistered. The S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14]. When requesting the user profile the S-CSCF can include the information in the P-Profile-Key header field in S-CSCF Registration/deregistration notification. When requesting the user profile, and the request received by the S-CSCF contains a P-Profile-Key header field, the S-CSCF can include the header field value in S-CSCF Registration/deregistration notification. If the response from the HSS includes a Wildcarded Public Identity AVP, and if the request received by the S-CSCF did not include a P-Profile-Key header field, the S-CSCF uses the AVP value to set the P-Profile-Key header field before forwarding the request to an AS.

Prior to performing S-CSCF Registration/Deregistration procedure with the HSS, the S-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] or use the value as received in the P-User-Database header field in the initial request for a dialog or a request for a standalone transaction as defined in RFC 4457 [82]. The HSS address received in the response to SLF query can be used to address the HSS of the public user identity with further queries.

If the HSS indicates to the S-CSCF that there is already another S-CSCF assigned for the user, the S-CSCF shall return a 305 (Use Proxy) response containing the SIP URI of the assigned S-CSCF received from the HSS in the Contact header field.

When the S-CSCF receives any response to the above request containing a Relayed-Charge header field, and the next hop is not an AS, the S-CSCF shall remove the Relayed-Charge header field.

When the S-CSCF receives any 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), the S-CSCF shall:

1) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed;

2) if the response is not forwarded to an AS (i.e. the response is related to a request that was matched to the first executed initial filter criteria):

a) remove the received "transit-ioi" header field parameter if present and insert a type 2 "term-ioi" header field parameter in the P-Charging-Vector header field of the outgoing response. The type 2 "term-ioi" header field is set to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter. Values of "orig-ioi" and "term-ioi" header field parameters in the received response are removed; and

b) if the S-CSCF supports using a token to identify the registration, remove the "+g.3gpp.registration-token" Feature-Caps header field parameter, defined in subclause 7.9A.8, if received in the response;

3) in case the served user is not considered a privileged sender then:

a) if the P-Asserted-Identity header field contains only a SIP URI and in the case where the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header field is an alias SIP URI for a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing this tel URI, including the display name associated with the tel URI, if available; and

b) if the P-Asserted-Identity header field contains only a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home network domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CSCF shall also add a "user" SIP URI parameter equals "phone" to the SIP URI;

4) in case the response is sent towards the originating user, the S-CSCF may retain the P-Access-Network-Info header field based on local policy rules and the destination user (Request-URI);

5) save an indication that GRUU routeing is to be performed for subsequent requests sent within this same dialog if:

a) there is a record-route position saved as part of the initial dialog request state; and

b) the contact address in the response is a valid GRUU assigned by the S-CSCF as specified in subclause 5.4.7A.4 or a temporary GRUU self assigned by the UE based on the "temp-gruu-cookie" header field parameter provided to the UE;

6) if the S-CSCF supports using a token to identify the registration and if a registration exists, add a "+g.3gpp.registration-token" Feature-Caps header field parameter, as defined in subclause 7.9A.8, set to the same value as included in the "+g.3gpp.registration-token" Contact header field parameter of the third party REGISTER request sent to the AS when the UE registered; and

NOTE 28: There could be several responses returned for a single request, and the decision to insert or modify the Record-Route needs to be applied to each. But a response might also return to the S-CSCF multiple times as it is routed back through AS. The S-CSCF will take this into account when carrying out step 5) to ensure that the information is stored only once.

7) if the response is forwarded within the S-CSCF home network and not to an AS, insert a P-Charging-Function-Addresses header field populated with values received from the HSS.

When the S-CSCF receives a response to a request for a standalone transaction (whether the user is registered or not), then:

1) in case the served user is not considered a privileged sender then:

a) if the P-Asserted-Identity header field contains only a SIP URI and in the case where the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header field is an alias SIP URI for a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing this tel URI, including the display name associated with the tel URI, if available; and

b) if the P-Asserted-Identity header field contains only a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home network domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CSCF shall also add a "user" SIP URI parameter equals "phone" to the SIP URI; and

2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field; otherwise, the S-CSCF shall remove the access-network-charging-info parameter in the P-Charging-Vector header field.

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall:

1) insert a P-Charging-Function-Addresses header field populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards an AS;

1A) if the S-CSCF supports using a token to identify the registration and if a registration exists, add a "+g.3gpp.registration-token" Feature-Caps header field parameter, as defined in subclause 7.9A.8, set to the same value as included in the "+g.3gpp.registration-token" Contact header field parameter of the third party REGISTER request sent to the AS when the UE registered;

1B) if the S-CSCF supports using a token to identify the registration in case the response is not forwarded to an AS the S-CSCF shall remove the "+g.3gpp.registration-token" Feature-Caps header field parameter, defined in subclause 7.9A.8, if received in the response; and

2) if the response is not forwarded to an AS (i.e. the response is related to a request that was matched to the first executed initial filter criteria), remove the received "orig-ioi", "term-ioi" and "transit-ioi" header field parameter if present and insert a type 2 "term-ioi" header field parameter in the P-Charging-Vector header field of the outgoing response. The type 2 "term-ioi" header field parameter is set to a value that identifies the sending network of the response and the type 2 "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter.

NOTE 29: If the S-CSCF forked the request of a stand alone transaction to multiple UEs and receives multiple 200 (OK) responses, the S-CSCF will select and return only one 200 (OK) response. The criteria that the S-CSCF employs when selecting the 200 (OK) response is based on the operator's policy (e.g. return the first 200 (OK) response that was received).

When the S-CSCF receives, destined for a served user, a target refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

0) if the dialog is related to an IMS communication service determine whether the contents of the request (e.g. SDP media capabilities, Content-Type header field) match the IMS communication service as received as the ICSI value in the P-Asserted-Service header field in the initial request. As an operator option, if the contents of the request do not match the IMS communication service the S-CSCF may reject the request by generating a status code reflecting which added contents are not matching. Otherwise, continue with the rest of the steps;

1) if the incoming request is received on a dialog for which GRUU routeing is to be performed and the Request-URI is not the GRUU for this dialog, then return a response of 400 (Bad Request).

2) if the incoming request is received on a dialog for which GRUU routeing is to be performed and the Request-URI contains the GRUU for this dialog then:

i) if the Request-URI contains a valid GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that does not contain a "bnc" URI parameter, then perform the procedures for Request Targeting specified in RFC 5627 [93], using the public user identity and instance ID derived from the Request-URI, as specified in subclause 5.4.7A;

ii) if the Request-URI contains a valid public GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that contains a "bnc" URI parameter then the target set is determined by following the procedures for routeing of public GRUUs specified in RFC 6140 [191]. or

NOTE 30: The procedures for Request Targeting for public GRUUs in subclause 7.1.1 of RFC 6140 [191] involve copying the "sg" SIP URI parameter from the Public GRUU into the Request-URI along with the bound registered Contact Address.

iii) if the Request-URI contains a temporary GRUU not assigned by the S-CSCF but that contains "temp-gruu-cookie" information provided by the S-CSCF to the UE in a "temp-gruu-cookie" header field parameter as specified in RFC 6140 [191] then the target set is determined by following the procedures for routeing of temporary GRUUs specified in RFC 6140 [191];

NOTE 31: The procedures for obtaining the "temp-gruu-cookie" information from the temporary GRUU and for routeing of temporary GRUUs are specified in subclause 7.1.2.3 of RFC 6140 [191].

iv) if no contact can be selected, return a response of 480 (Temporarily Unavailable);

3) remove its own URI from the topmost Route header field;

4) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), save the Contact and CSeq header field values received in the request such that the S-CSCF is able to release the session if needed;

5) create a Record-Route header field containing its own SIP URI;

5A) void

5B) if the request was sent on a dialog for which logging of signalling is in progress, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred, stop treating the dialog as one for which logging of signalling is in progress, else append a "logme" header field parameter to the SIP Session-ID header field if the parameter is missing and determine, by checking its trace configuration, whether to log the request; and

6) forward the request based on the topmost Route header field.

When the S-CSCF receives any response to the above request, the S-CSCF shall:

1) If the response contains a "logme" header field parameter in the SIP Session-ID header field then log the response based on local policy.

When the S-CSCF receives any 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

1) for INVITE dialogs, replace the saved Contact header field values in the response such that the S-CSCF is able to release the session if needed; and

2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field; otherwise, the S-CSCF shall remove the access-network-charging-info parameter in the P-Charging-Vector header field.

When the S-CSCF receives, destined for the served user, a subsequent request other than target refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

1) if the incoming request is received on a dialog for which GRUU routeing is to be performed and the Request-URI is not the GRUU for this dialog, then return a response of 400 (Bad Request).

2) if the incoming request is received on a dialog for which GRUU routeing is to be performed and the Request-URI contains the GRUU for this dialog then:

i) if the Request-URI contains a valid GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that does not contain a "bnc" URI parameter, then perform the procedures for Request Targeting specified in RFC 5627 [93], using the public user identity and instance ID derived from the Request-URI, as specified in subclause 5.4.7A;

ii) if the Request-URI contains a valid public GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that contains a "bnc" URI parameter then the target set is determined by following the procedures for routeing of public GRUUs specified in RFC 6140 [191]; or

NOTE 32: The procedures for Request Targeting for public GRUUs in subclause 7.1.1 of RFC 6140 [191] involve copying the "sg" SIP URI parameter from the Public GRUU into the Request-URI along with the bound registered Contact Address.

iii) if the Request-URI contains a temporary GRUU not assigned by the S-CSCF but that contains "temp-gruu-cookie" information provided by the S-CSCF to the UE in a "temp-gruu-cookie" header field parameter as specified in RFC 6140 [191] then the target set is determined by following the procedures for routeing of temporary GRUUs specified in RFC 6140 [191].

NOTE 33: The procedures for obtaining the "temp-gruu-cookie" information from the temporary GRUU and for routeing of temporary GRUUs are specified in subclause 7.1.2.3 of RFC 6140 [191].

iv) if no contact can be selected, return a response of 480 (Temporarily Unavailable).

3) remove its own URI from the topmost Route header field;

3A) void

3B) if the request was sent on a dialog for which logging of signalling is in progress, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred, stop treating the dialog as one for which logging of signalling is in progress, else append a "logme" header field parameter to the SIP Session-ID header field if the parameter is missing and determine, by checking its trace configuration, whether to log the request; and

4) forward the request based on the topmost Route header field.

When the S-CSCF receives any response to the above request, the S-CSCF shall:

1) If the response contains a "logme" header field parameter in the SIP Session-ID header field then log the response based on local policy.

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the access-network-charging-info parameter from the P-Charging-Vector header field; otherwise, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header field.

With the exception of 305 (Use Proxy) responses, the S-CSCF shall not recurse on 3xx responses.

\*\*\*\*\* Fifth change \*\*\*\*\*

### 5.5.1 General

The MGCF, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem. Therefore table A.4/1 and dependencies on that major capability shall not apply.

The use of the Path and Service-Route header fields shall not be supported by the MGCF.

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the MGCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the MGCF shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the MGCF sends any request or response related to a dialog, the MGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses header fields before sending the message.

The MGCF shall use a GRUU referring to itself (as specified in RFC 5627 [93]) when inserting a contact address in a dialog establishing or target refreshing SIP message. This specification does not define how GRUUs are created by the MGCF; they can be provisioned by the operator or obtained by any other mechanism. A GRUU used by the MGCF when establishing a dialog shall remain valid for the lifetime of the dialog. The GRUU used by the MGCF shall not reveal calling party related information.

The MGCF shall handle requests addressed to its currently valid GRUUs when received outside of the dialog in which the GRUU was provided.

EXAMPLE: Upon receipt of an INVITE request addressed to a GRUU assigned to a dialog it has active, and containing a Replaces header field referencing that dialog, the MGCF will be able to establish the new call replacing the old one.

The MGCF may support retrieval of NP data, subject to local policy. The interface used at the MGCF to retrieve the NP data is out of scope of this specification. Retrieval of NP data is relevant only if the Request-URI contains an international public telecommunications number. For requests from the IM CN subsystem network, if the Request-URI contains a tel-URI with an "npdi" tel-URI parameter, as defined in RFC 4694 [112], NP data has been obtained previously and NP data retrieval is not needed, but still may still be performed if required by local policy. If NP data is retrieved by the MGCF, and the request is routed to the IM CN subsystem, the MGCF shall add the tel-URI NP parameters to the Request-URI as defined in RFC 4694 [112]: an "npdi" tel-URI parameter is added to indicate that NP data retrieval has been performed, and if the number is ported, an "rn" tel-URI parameter is added to identify the ported-to routeing number.

The MGCF NP procedures also apply when the request contains a Request-URI in the form of a SIP URI user=phone, where the "npdi" and "rn" tel-URI parameters are contained in the userinfo part of the SIP URI.

The MGCF supports as a network option the inclusion of the XML MIME schema for PSTN. In cases where the XML MIME for PSTN is included the Content-Type header field is set to "application/vnd.etsi.pstn+xml" and the Content-Disposition to "signal" with the "handling" parameter set to "optional".

The MGCF shall log all SIP requests and responses that contain a "logme" header field parameter in the SIP Session-ID header field if required by local policy.

When sending a failure response to any received request, depending on operator policy, the MGCF may insert a Response-Source header field with an "fe" header field parameter constructed with the URN namespace "urn:3gpp:fe", the fe-id part of the URN set to "mgcf" and optionally an appropriate fe-param part of the URN set in accordance with subclause 7.2.17.

\*\*\*\*\* Sixth change \*\*\*\*\*

### 5.6.1 General

The use of the Path and Service-Route header fields shall not be supported by the BGCF.

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the BGCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the BGCF shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the BGCF receives any request or response related to a dialog or standalone transaction, the BGCF may insert previously saved values into a P-Charging-Vector header field before forwarding the message.

When the BGCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the BGCF may insert previously saved values into a P-Charging-Function-Addresses header field before forwarding the message.

With the exception of 305 (Use Proxy) responses, the BGCF may recurse on a 3xx response only when the domain part of the URI contained in the 3xx response is in the same domain as the BGCF. For the same cases, if the URI is an IP address, the BGCF shall only recurse if the IP address is known locally to be a address that represents the same domain as the BGCF.

The BGCF shall log all SIP requests and responses that contain a "logme" header field parameter in the SIP Session-ID header field if required by local policy.

When sending a failure response to any received request, depending on operator policy, the BGCF may insert a Response-Source header field with an "fe" header field parameter constructed with the URN namespace "urn:3gpp:fe", the fe-id part of the URN set to "bgcf" and optionally an appropriate fe-param part of the URN set in accordance with subclause 7.2.17.

\*\*\*\*\* Seventh change \*\*\*\*\*

### 5.7.2 Application Server (AS) acting as terminating UA, or redirect server

When acting as a terminating UA the AS shall behave as defined for a UE in subclause 5.1.4, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

If the AS requires knowledge of the served user it shall determine the served user according to the applicable procedure in subclause 5.7.1.3A.

An AS acting as redirect server shall propagate any received IM CN subsystem XML message body in the redirected message.

When an AS acting as a terminating UA generates a subsequent request for a dialog, the AS shall insert a P-Charging-Vector header field with the "icid-value" header field parameter set to the value populated in the initial request for the dialog and a type 3 "orig-ioi" header field parameter. The AS shall set the type 3 "orig-ioi" header field parameter to a value that identifies the service provider from which the request is sent. The AS shall not include the type 3 "term-ioi" header field parameter.

When the AS acting as terminating UA receives a request, the AS shall store the value of the "orig-ioi" header field parameters received in the P-Charging-Vector header field if present.

NOTE 1: Any received orig-ioi parameter will be a type 3 orig-ioi. The orig-ioi identifies the network operator from which the request was sent.

When the AS acting as terminating UA generates a response to a request, the AS shall insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the request, a type 3 "term-ioi" header field parameter and the "icid-value" header field parameter. The AS shall set the type 3 "term-ioi" header field parameter to a value that identifies the service provider from which the response is sent, the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter and the "icid-value" header field parameter is set to the previously received value of "icid-value" header field parameter in the request.

The AS acting as terminating UA receiving an initial request with a P-Charging-Vector header field shall, based on local policy, store the "fe-identifier" header field parameter of the P-Charging-Vector header field.

The AS acting as terminating UA shall, based on local policy, include the stored "fe-identifier" header field parameter in the P-Charging-Vector header field, add its address or identifier and application id to the "as-addr" and "as-id" elements of the "fe-identifier" header field parameter of the P-Charging-Vector header field and send the P-Charging-Vector header field in the related final response.

NOTE 2: An AS hosting multiple applications can add multiple pairs of "as-addr" and "as-id" header field parameters when executing these applications.

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the AS shall include the Resource-Priority header field in all requests associated with that dialog. If priority is supported, the AS shall take into account that subsequent received SIP requests or responses within the same dialog or transaction may have added or changed the Resource-Priority header field or backwards indication.

NOTE 3: An AS can modify the priority using the Resource-Priority header field in a dialog on behalf of a user. The mechanism for a user to invoke this AS action is out of scope of this release of the specification.

\*\*\*\*\* Eighth change \*\*\*\*\*

### 5.7.3 Application Server (AS) acting as originating UA

In order to support an AS acting as an originating UA, the AS has to be within the same trust domain as the S-CSCF to which requests will be sent.

When acting as an originating UA the AS shall behave as defined for a UE in subclause 5.1.3, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses and does not participate in any authentication procedures defined for a UE. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall insert a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17] and a type 3 "orig-ioi" header field parameter. The AS shall set the type 3 "orig-ioi" header field parameter to a value that identifies the service provider from which the request is sent. The AS shall not include the type 3 "term-ioi" header field parameter.

NOTE 1: The AS can retrieve CDF and/or ODF addresses from HSS on Sh interface.

When the AS acting as an originating UA receives any response to a request, the AS shall store the value of the "term-ioi" header field parameter received in the P-Charging-Vector header field if present.

NOTE 2: Any received "term-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the network operator from which the response was sent.

When an AS acting as an originating UA generates a subsequent request for a dialog, the AS shall insert a P-Charging-Vector header field with the "icid-value" header field parameter set to the value populated in the initial request for the dialog and a type 3 "orig-ioi" header field parameter. The AS shall set the type 3 "orig-ioi" header field parameter to a value that identifies the service provider from which the request is sent. The AS shall not include the type 3 "term-ioi" header field parameter.

Based on local policy, the AS acting as an originating UA or application(s) hosted by the AS acting as originating UA shall add an "as-addr" and an "as-id" element of the "fe-identifier" header field parameter to the P-Charging-Vector header field with its own address or identifier and application identifier to an initial request.

NOTE 3: An AS hosting multiple applications can add multiple pairs of "as-addr" and "as-id" header field parameters when executing these applications for an initial request.

The AS shall extract charging function addresses from any P-Charging-Function-Addresses header field that is received in any 1xx or 2xx responses to the requests.

The AS may also indicate that the proxies should not fork the request by including a "no-fork" directive within the Request-Disposition header field in the request as described in RFC 3841 [56B].

When sending any initial request, an identity is needed that will correlate with the service profile to be used at the S-CSCF. If the identity for that service profile corresponds to the value to be used to identify the caller to the destination user, include the identity in the P-Asserted-Identity header field. If the identity for that service profile does not correspond to the value to be used to identify the caller to the destination user, and the P-Served-User header field is supported by the S-CSCF, include the identity in the P-Served-User header field. This leaves the P-Asserted-Identity header field for the identity to be used to identify the caller to the destination user. If the identity for that service profile matches a wildcarded identity and the P-Profile-Key header field is supported by the AS, include the wildcarded identity in the P-Profile-Key header field.

When sending an initial request on behalf of a PSI that is hosted by the AS, the AS shall:

- insert a Request-URI as determined by the service logic;

- insert a P-Asserted-Identity header field and possibly a P-Served-User header field containing the PSI as indicated earlier in this subclause;

- if the AS is not able to resolve the next hop address by itself or the operator policy does not allow it, insert a Route header field pointing either to the S-CSCF where the PSI is hosted, or to the entry point of the home network of the PSI or to the transit function. The AS shall append the "orig" parameter to the URI in the topmost Route header field; and

NOTE 4: The address of the S-CSCF hosting the PSI can be obtained by querying the HSS on the Sh interface.

NOTE 5: AS can only send the initial request to the entry point of the home network of the PSI only if the AS can assume (e.g. based on local configuration) that the receiving entry point will be able to process the request as an originating request.

- if the AS is able to resolve the next hop address by itself and the operator policy allows it, forward the originating request directly to the destination without involving any S‑CSCF in the originating IM CN subsystem.

When sending an initial request on behalf of a public user identity, the AS shall:

- insert a Request-URI as determined by the service logic;

- insert a P-Asserted-Identity header field and possibly a P-Served-User header field containing the public user identity as indicated earlier in this subclause;

- if the AS intends to send the originating request to the home network of the public user identity or the operator policy requires it, insert a Route header field pointing to the S-CSCF where the public user identity on whose behalf the request is generated is registered or hosted (unregistered case) or to the entry point of the public user identity's network. The AS shall append the "orig" parameter to the URI in the topmost Route header field; and

NOTE 6: The address of the S-CSCF can be obtained either by querying the HSS on the Sh interface or during third-party registration.

NOTE 7: AS can send the initial request to the entry point of the public user identity's network or to the entry point of the home network of the PSI only if the AS can assume (e.g. based on local configuration) that the receiving entry point will be able to process the request as an originating request.

- if the AS intends to send the originating request directly to the terminating network and the operator policy allows it, forward the originating request directly to the destination without involving any S‑CSCF in the originating IM CN subsystem.

When sending an initial request to a served public user identity, the AS shall insert:

- a Request-URI containing the served public user identity;

- a P-Asserted-Identity as determined by the service logic (e.g. the URI of the AS or the URI of the entity that triggered the SIP request, if the sending of the initial request is triggered by a non-SIP request); and

- a Route header field pointing to the S-CSCF where the public user identity to whom the request is generated is registered or hosted (unregistered case) or to the entry point of the public user identity's network. The AS shall not append the "orig" parameter to the URI in the topmost Route header field.

NOTE 8: The address of the S-CSCF can be obtained either by querying the HSS on the Sh interface or during third-party registration.

The AS can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the AS shall set a display-name of the From header field to "Anonymous" as specified in RFC 3261 [26] and set an addr-spec of the From header field to Anonymous User Identity as specified in 3GPP TS 23.003 [3].

NOTE 9: The contents of the From header field cannot be relied upon to be modified by the network based on any privacy specified by the user either within the AS indication of privacy or by network subscription or network policy. Therefore the AS includes the value "Anonymous" whenever privacy is explicitly required.

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the AS shall include the Resource-Priority header field in all requests associated with that dialog. If priority is supported, the AS shall take into account that subsequent received SIP requests or responses within the same dialog or transaction may have added or changed the Resource-Priority header field or backwards indication.

NOTE 10: An AS can modify the priority using the Resource-Priority header field in a dialog on behalf of a user. The mechanism for a user to invoke this AS action is out of scope of this release of the specification.

\*\*\*\*\* Ninth change \*\*\*\*\*

### 5.8.1 General

Although the MRFC is acting as a UA, it is outside the scope of this specification how the MRFC associated addresses are made known to other entities.

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the MRFC shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the MRFC shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE: This special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the MRFC sends any request or response (excluding CANCEL requests and responses) related to a dialog or standalone transaction, the MRFC may insert previously saved values into P-Charging-Vector header field before sending the message.

When the MRFC sends any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the MRFC may insert previously saved values into P-Charging-Function-Addresses header fields before sending the message.

The MRFC shall use a GRUU referring to itself (as specified in RFC 5627 [93]) when inserting a contact address in a dialog establishing or target refreshing SIP message. This specification does not define how GRUUs are created by the MRFC; they can be provisioned by the operator or obtained by any other mechanism. A GRUU used by the MRFC when establishing a dialog shall remain valid for the lifetime of the dialog.

The MRFC shall handle requests addressed to its currently valid GRUUs when received outside of the dialog in which the GRUU was provided.

EXAMPLE: Upon receipt of an INVITE request addressed to a GRUU assigned to a dialog it has active, and containing a Replaces header field referencing that dialog, the MRFC will be able to establish the new call replacing the old one.

The MRFC shall log all SIP requests and responses that contain a "logme" header field parameter in the SIP Session-ID header field if required by local policy.

When sending a failure response to any received request, depending on operator policy, the MRFC may insert a Response-Source header field with an "fe" header field parameter constructed with the URN namespace "urn:3gpp:fe", the fe-id part of the URN set to "mrfc" and optionally an appropriate fe-param part of the URN set in accordance with subclause 7.2.17.

\*\*\*\*\* Tenth change \*\*\*\*\*

## 5.8A Procedures at the MRB

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the MRB shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the MRB shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE: This special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

The MRB shall log all SIP requests and responses that contain a "logme" header field parameter in the SIP Session-ID header field based on local policy.

\*\*\*\*\* Eleventh change \*\*\*\*\*

#### 5.10.2.1A General

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the IBCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the IBCF shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE 1: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

Based on local policy, the IBCF acting as an exit point shall add in responses in the P-Charging-Vector header field a "transit-ioi" header field parameter with an entry which identifies the operator network which the response is transitting or with a void entry.

Based on local policy the IBCF shall delete or void in responses in the P-Charging-Vector header field any received "transit-ioi" header field parameter value.

If an IBCF in the originating visited network, supporting barring of premium numbers when roaming, receives a request to be sent towards the originating home network and the request is originated from a roaming UE and the Request-URI contains an E.164 number encoded as described in subclause 5.1.2A.1.2 which the IBCF is able to identify as a premium rate number in the country of the served network, the IBCF shall, based on local policy, add the "premium-rate" tel URI parameter specified in subclause 7.2A.17 set to a value "information" or "entertainment" as appropriate.

NOTE 2: The feature barring of premium numbers when roaming can be implemented in the P-CSCF or an IBCF of the visited network. Local policy ensures that the feature is only activiated in one of the two.

NOTE 3: If the visited network supports indicating traffic leg as specified in RFC 7549 [225] the above request includes the "iotl" SIP URI parameter with the value "visitedA-homeA" in the bottommost Route header field.

\*\*\*\*\* Twelfth change \*\*\*\*\*

#### 5.13.2.2 General

This subclause applies for requests sent from the S-CSCF to the AS via the ISC gateway function.

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field, the ISC gateway function shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the ISC gateway function shall adjust the priority treatment of transactions or dialogs according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

\*\*\*\*\* Thirteenth change \*\*\*\*\*

# I.1A General

For all SIP transactions identified, if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field. The additional routeing functionality shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If priority is supported, the priority treatment of transactions or dialogs shall be adjusted according to the most recently received authorized Resource-Priority header field or backwards indication value.

NOTE 1: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

NOTE 2: These SIP transactions are exempt from network management controls.

If logging is in progress for this dialog, check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K]. If a stop trigger event has occurred then stop logging of signalling, else determine, by checking its debug configuration, whether to log the response.

With the exception of 305 (Use Proxy) responses, the additional routeing functionality shall not recurse on 3xx responses.

If the additional routeing functionality inserts its own Record-Route header field, then the additional routeing functionality may require the periodic refreshment of the session to avoid hung states. If the network element requires the session to be refreshed, the additional routeing functionality shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 3: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

Based on local policy the additional routeing function shall add in requests and in responses in the P-Charging-Vector header field a "transit-ioi" header field parameter with an entry which identifies the operator network which the request or response is transitting or with a void entry.

Based on local policy the additional routeing function shall delete or void in requests and in responses in the P-Charging-Vector header field any received "transit-ioi" header field parameter value.