3GPP TR 23.808 V1.0.1 (2006-05)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Supporting Globally Routable User Agent URI in IMS;
Report and Conclusions
(Release 7)

Keywords

Global Routable User Agent, GRUU, Instance ID

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document is a temporary container for the architectural impacts on IM CN subsystem for supporting GRUU. The contents of this report when stable will be the base for CRs to 3GPP Technical Specifications e.g. TS 23.228 [2].

GRUU is a URI, the creation and use of which is defined in an IETF specification draft-ietf-sip-gruu-0 [1] in order to route SIP messages to a specific SIP User Agent (UA) instance. The support of GRUU in IMS is to enable routing of SIP messages to a specific instance of a registered public user identity even when a single public user id is registered from multiple UEs.

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] draft-ietf-sip-gruu-0 (March 2006): "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)", work in progress.

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[2] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[3] 3GPP TS 23.279: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services; Stage 2".

[4] draft-ietf-sipping-gruu-reg-event-03.txt (February 2006): "Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routeable User Agent URIs (GRUUs)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[5] 3GPP TS 33.203: "Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Instance identifier: It is an identifier, represented with a URN,that uniquely identifies a SIP user agent amongst all other user agents associated with an AOR e.g. public user id.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

GRUU	Globally Routable User Agent (UA) URI
URN	Uniform Resource Name
AOR	Address of Record

4 Relationship between Services and GRUU

4.1 Analysis of IMS functions requiring GRUU

The IMS architecture supports the possibility for multiple UEs to register with the same Public User Identity. However since current IMS addressing and routing is based solely on Public User Identities this can result in SIP requests in IMS being forked to multiple contacts when more than on UE is registered with the same Public User Identity. For some IMS applications this forking to multiple contacts registered with the same Public User Identity is not always a desirable behaviour when what is needed is a mechanism to identify and route to a specific UE instance.

Many IMS based applications need to be able to identify the origin of and route SIP signalling to a specific UE instance even when multiple UEs use the same Public User Identity. The IETF GRUUs (Globally Routable User Agent URIs) offers a solution to this problem. A GRUU URI enables routing to a specific user agent instance. There are several IMS applications where the GRUU properties may be needed in order for the application to operate correctly:

- **Combinational Services**

  In the Combinational Services TS 23.279 [3] User A may be in a CS call with User B and User A needs to determine the IMS capabilities of User B's UE by sending a SIP OPTIONS request to the specific UE instance of User B that User A is involved in the CS call with. If User B has multiple terminals with the same E.164 number IMS Registered then the response to the SIP OPTIONS request may not be that from the UE that User B is using for the CS call. This causes the UE A's capabilities record for User B to be invalid. Likewise if User A attempts to establish an IMS Messaging Session to User B while in a CS call the IMS Messaging Session SIP INVITE request needs to be addressed to the specific UE instance that User B is using for the CS call. In order to ensure this works when User B has multiple terminals with the same E.164 number IMS Registered the URI in the destination address of this SIP INVITE request needs to be a GRUU.

Editor's note: For Combinational Services a solution for the forking problem is already described in TS 23.279 [3]. This solution uses a Personal ME Identifier registered by the UE. It is FFS whether Combinational Services will use the GRUU concept at all and if so, how interoperability of the two approaches is assured.

- **Voice Call Continuity**

  Similar to Combinational Services, Voice Call Continuity requires that an IMS Session can be established with the same specific UE instance that is involved in an existing CS call. SIP requests in IMS need to be addressed to a specific Public User Identity and UE combination in order to avoid the CS call being handed over to a different UE instance that is registered with the same Public User Identity other than the one involved in the CS call. To ensure correct handover from CS to IMS the SIP requested need to be addressed to a GRUU.

- **Call Transfer Supplementary Service**

  In a Call Transfer when User A is talking to User B. User A wants to transfer the call to User C. So, User A sends a SIP REFER request to User C. That SIP REFER request contains a Refer-To header field that needs to contain a URI that can be used by User C to place a call to User B. However, this call needs to route to the specific UE instance which User B is using to talk to User A. If User B has multiple UEs registered with the same Public User Identity then currently in IMS, the Call Transfer Supplementary Service will not execute properly as all the UEs registered by User B with the same Public User Identity will be contacted. The URI provided by User B to User A in the Refer-To header needs to be a GRUU that uniquely identifies the specific Public User Identity and UE instance in order for the Call Transfer Supplementary Service to work properly. Supplementary IMS Services are needed for Fixed Broadband Access to IMS, Voice Call Continuity and for Multimedia Telephony work items. Another use case is for user B to transfer his call to another device he has.

- **Presence Service**

In the Presence System, the Presence Server generates notifications about the state of a user. This state is represented with the Presence Information Document Format (PIDF). In a PIDF document, a user is represented by a series of tuples, each of which describes the services that the user has. Each tuple also has a URI in the <contact> element, which is a SIP URI representing that device. A watcher can attempt a communication to that URI, with the expectation that the communication is routed to the service whose presence is represented in the tuple. In some cases where the publishing user has multiple UEs registered with the same Public User Identity the service represented by a tuple may exist on only a single UE associated with a user. In such a case, the URI in the presence document has to route to that specific UE instance and therefore this URI needs to be a GRUU.

- **Push to Talk over Cellular (PoC)**

OMA requirements for PoC V2.0 require that multiple PoC Clients with the same PoC Address are supported. In addition these requirements require that the PoC Service Settings (Answer Mode, Session Barring etc) that are published to the PoC Server using SIP PUBLISH are treated separately for each PoC Client with the same PoC Address and that invitations to PoC Sessions are each handled separately according to the PoC Settings of each PoC Client. This requires that the published PoC settings are identified by a GRUU that can be used to individually address SIP INVITE requests with the appropriate parameters based on the PoC Settings to each PoC Client instance.

4.2 Services Impacted by GRUU

4.2.1 Service behaviours for GRUUs

A SIP request addressed to a GRUU should be provided with terminating services, in the same way that requests addressed to a Public User Identity are provided services. There will be some cases where the same services should apply, whether the request is addressed to a GRUU or a Public User Identity. For example, if a user has terminating call blocking based on caller identity, then the same blocking treatment should be applied whether the request is addressed to the Public Identity or the GRUU. There are also cases where requests addressed to a GRUU should receive different services than requests addressed to the Public Identity. For example, if a user activates call-forwarding-all-calls, then requests routed to the Public User Identity should be forwarded, while requests addressed to the GRUU should not be forwarded since these call are addressed to a specific UE instance.

A user may have a service such as call blocking that is applied even when the user is unregistered. Providing the same treatment to the blocked caller for both the registered and unregistered case prevents disclosure of registration status to the blocked user. The effect should be the same when the blocked caller uses a GRUU.

4.2.2 Mechanisms for enabling service behaviour for GRUUs

Whether a Request URI is a GRUU or not can be easily tested, since a GRUU will always contain the parameter 'gruu'. iFCs, by default, may test for presence of special parameter in the Request URI. The iFCs in the profile may test for the presence of a 'gruu' URI parameter in the request URI of a message and selectively apply services that are only applicable for GRUUs.

5 Overall Architecture Requirements for support of GRUU

5.1 General Requirements

5.2 Architecture Requirements

The solution for support of GRUU in the IMS should fulfil the following architectural requirements:

1. A GRUU shall be registered in the IMS network with a unique combination of specific Public User Identity and UE.

2. A UE shall be able to request a GRUU that is associated with a specific Public User Identity at a specific UE at the time of registration of the Public User Identity.

3. The IMS network shall be able to receive a request for generation of a GRUU for a specific Public User Identity at a specific UE instance and be able to generate such a GRUU and send it back to the UE that requested it.

4. The IMS network shall be able to reject a request to generate a GRUU because the IMS network is an earlier release that has no support for the ability to generate a GRUU.

5. When the IMS network receives a request to generate a GRUU for a specific Public User Identity, the IMS network shall also generate GRUUs for all implicitly registered Public User Identities belonging to the same implicit registration set. The IMS network shall communicate all these other GRUUs to the UE.

6. The IMS network always generates the same GRUU for a given Public User Identity and Instance Identifier combination.

7. The IMS network shall be able to derive the Public User Identity directly from the GRUU. The public user identity derived from the GRUU used to identify the contact address of the sender shall be same as the public user identity used to identify the initiator or an associated Public User Identity, i.e. the public user identity derived from GRUU conveyed in the SIP Contact header shall be the same as the public user identity conveyed in the SIP P-Asserted-Identity header or be in an implicit registration set with that one. If the URI in the SIP Contact header of the sender carries a parameter indicating that it is a GRUU but does not comply with the stated requirement or if there is no registration corresponding to the GRUU, then the IMS network should reject the request.

Editors note: The procedure of how to handle the case when these two identities are not same is for FFS.

8. The IMS network shall be able to route requests destined to a GRUU to the UE instance registered with that GRUU.The IMS network does not fork SIP requests addressed to a GRUU.

9. The IMS network will be able to generate a GRUU for any UE registered with a valid SIP or TEL URI.

10. A UE that is capable of supporting GRUUs shall be able to differentiate between a GRUU and a Public User ID.

11. A UE shall be able to establish a session or non-session related communication with another UE using a GRUU.

12. A UE supporting GRUUs shall be able to inter-work with an IMS network not supporting GRUUs.

13. A UE supporting GRUUs shall be able to inter-work with an UE not supporting GRUUs.

14. A UE or network that does not support GRUUs shall not be negatively affected when communicating with a network or UE supporting GRUUs.

15. It shall be possible to define iFCs that match the Public User Identity part of a GRUU.

16. As all registrations pertaining to a particular Public User Identity are directed to the same S-CSCF, registrations of all GRUUs associated with a specific Public User Identity shall also be directed to the same S-CSCF.

17. The GRUU format shall comply with the specifications of GRUU draft [1].

5.3 Security Requirements

The solution for support of GRUU in the IMS should fulfil the following architectural requirements:

1. It shall be possible to apply same level of privacy irrespective whether GRUU is used or not.

2. It shall be possible to apply same level of security irrespective whether GRUU is used or not.

5.4 Charging Requirements

Editors note: Contains any charging considerations that need to be taken into account when a GRUU is used.

6 Impacts on UE and on the IM CN subsystem

Editor's Note: Impacts related to support security requirements for GRUU are FFS.

6.1 UE

A UE supporting GRUU mechanism and wishing to request a GRUU during registration shall indicate the support for the GRUU mechanism in the registration request and retain the GRUU in the registration response. The UE should generate an instance identifier that is unique across other UEs that have registered with the same IMPU, as specified in the architecture requirements. Guidance for generation of instance identifiers is found in draft-ietf-sip-gruu-07.txt and draft-ietf-sip-outbound-02.txt. It is recommended that a UE not use IMS private user identity as instance identifier.

When UE wishes to request a GRUU during registration it shall add an instance identifier in the registration request such that the instance id is unique across other registrations of the same public user identity.

If the registered Public User Identity is part of an implicit registration set, the UE must also obtain and retain the GRUU for each implicitly registered Public User Identity which would be sent by the S-CSCF in accordance to [4].

6.1.2 Using a GRUU

When sending SIP requests from an explicitly or implicitly registered Public User Identity for which a UE obtained GRUU, the UE shall use the corresponding retained GRUU as a Contact address, rather than the contact address that UE sent in the registration request.

When responding to SIP requests where the P-Called-Party is a registered Public User Identity Identity for which a UE obtained GRUU, the UE must use the corresponding retained GRUU as a Contact address, rather than the contact address that was registered.

Any UE may learn a GRUU of another UE using mechanisms that are outside the scope of this specification. A UE may learn a GRUU from the contact header of a request, from presence information, or by other mechanisms.

Since a GRUU can be used as a Request URI wherever a Request URI would normally be inserted, a UE that issues a request towards a GRUU does not necessarily need to support the GRUU mechanism itself.

If a UE has subscribed to the reg event package, and subsequently receives a notification indicating that an implicit registration has occurred for a contact the UE has registered, then the UE must retain GRUUs from the notification for future use.

6.1.3 Using a GRUU while requesting Privacy

When a UE sends a request or response containing a GRUU, and it wishes to block the delivery of its Public User Identity to an untrusted destination, it must include a 'Privacy' header containing both the 'header' and 'id' tokens.

6.2 Core Network Entities

6.2.1 HSS

There are no changes to HSS procedures when using a GRUU. When routing requests addressed to a GRUU to the terminating S-CSCF, the I-CSCF removes any URI parameters from the Request URI before querying the HSS. When the Request URI is a GRUU this has the effect of deriving the Public Identity from the GRUU and hence does not impact the HSS.

6.3 IP Multimedia (IM) Core Network (CN) Subsystem entities

6.3.1 P-CSCF

There are no changes to the P-CSCF procedures due to GRUU.

6.3.2 S-CSCF

6.3.2.1 Allocating a GRUU during registration

The S-CSCF, when receiving a registration request from a UE that includes an instance id, shall allocate a GRUU. If the UE indicates support of GRUU in the REGISTER request, then the S-CSCF shall return the GRUU in the registration response and record that GRUU supported by UE. The GRUU shall be formed by adding two URI parameters to the public user identity: a 'gruu' parameter with no value, and an 'opaque' parameter with a value containing the instance id . For example, if the public user id is given by *sip:bob@3gpp.org* then the GRUU is given by *sip:bob@3gpp.org;gruu;opaque="urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"* where the opaque parameter uniquely identifies the instance.

NOTE: As long as the instance id provided in the register request is the same, the resulting GRUU will always be the same for a given public user identity.

If there are implicitly registered public user identities, the S-CSCF shall generate a GRUU for each implicitly registered public user identity.

When sending notification for the registration event package, the S-CSCF shall use the extension defined in [4] to include the GRUU for each registered Contact that has been assigned a GRUU.

6.3.2.2 Using a GRUU

There are no added impacts on S-CSCF for execution of services for GRUUs The iFCs in the profile may test for the presence of a 'gruu' URI parameter in the Request URI of a message . The S-CSCF validates the GRUU and passes the SIP message with the validated GRUU to application servers based the iFC trigger. Application servers can then apply services to the GRUU.

Editor's Note: Whether the S-CSCF need check the GRUU conveyed in the SIP contact header is FFS.

If the SIP message is destined to a GRUU, then the S-CSCF shall associate the request with the corresponding public user identity. The S-CSCF will not fork this request, but will direct the call to the identified instance.

S-CSCF shall provide an indication to UE that the SIP request was targeted to GRUU.

6.3.3 I-CSCF

No changes to the I-CSCF are required to support GRUU. When routing requests addressed to a GRUU to the terminating S-CSCF, the I-CSCF removes any URI parameters from the request URI before querying the HSS. When the request URI is a GRUU this has the effect of deriving the Public Identity from the GRUU. Messages routed to the terminating S-CSCF include the URI parameters.

7 Procedures for GRUU

Editors note: Contains impacts to information flows in the IMS sub-system. Will contain only those flows from TS 23.228 that are being modified and updates suggested to those flows with change-bars.

7.1 Registration flows

7.1.1 Requirements to consider for registration

The additional requirement for the registration information flow for this section is:

1. A Serving CSCF is assigned at registration, this does not preclude additional Serving CSCFs or change of CSCF at a later date. Procedures for use of additional CSCFs are not standardised in this release.

7.1.2 Assumptions

The following are considered as assumptions for the registration procedures as described in clause 5.3.2.3:

1. IP-CAN bearer is already established for signalling and a mechanism exists for the first REGISTER message to be forwarded to the proxy.

2. The I-CSCF shall use a mechanism for determining the Serving CSCF address based on the required capabilities. The I-CSCF obtains the name of the S-CSCF from its role as an S-CSCF selector (figure 7.1) for the determination and allocation of the Serving CSCF during registration.

3. The decision for selecting the S-CSCF for the user in the network is made in the I-CSCF.

4. A role of the I-CSCF is the S-CSCF selection.

In the information flows described in clauses 7.1.3 and 7.1.4, there is a mechanism to resolve a name and address. The text in the information flows indicates when the name-address resolution mechanism is utilised. These flows do not take into account security features such as user authentication. The description of the impact of IMS security features is done in TS 33.203 [5].

7.1.3 Registration information flow – User not registered

The application level registration can be initiated after the registration to the access is performed, and after IP connectivity for the signalling has been gained from the access network. For the purpose of the registration information flows, the user is considered to be always roaming. For user roaming in their home network, the home network shall perform the role of the visited network elements and the home network elements.

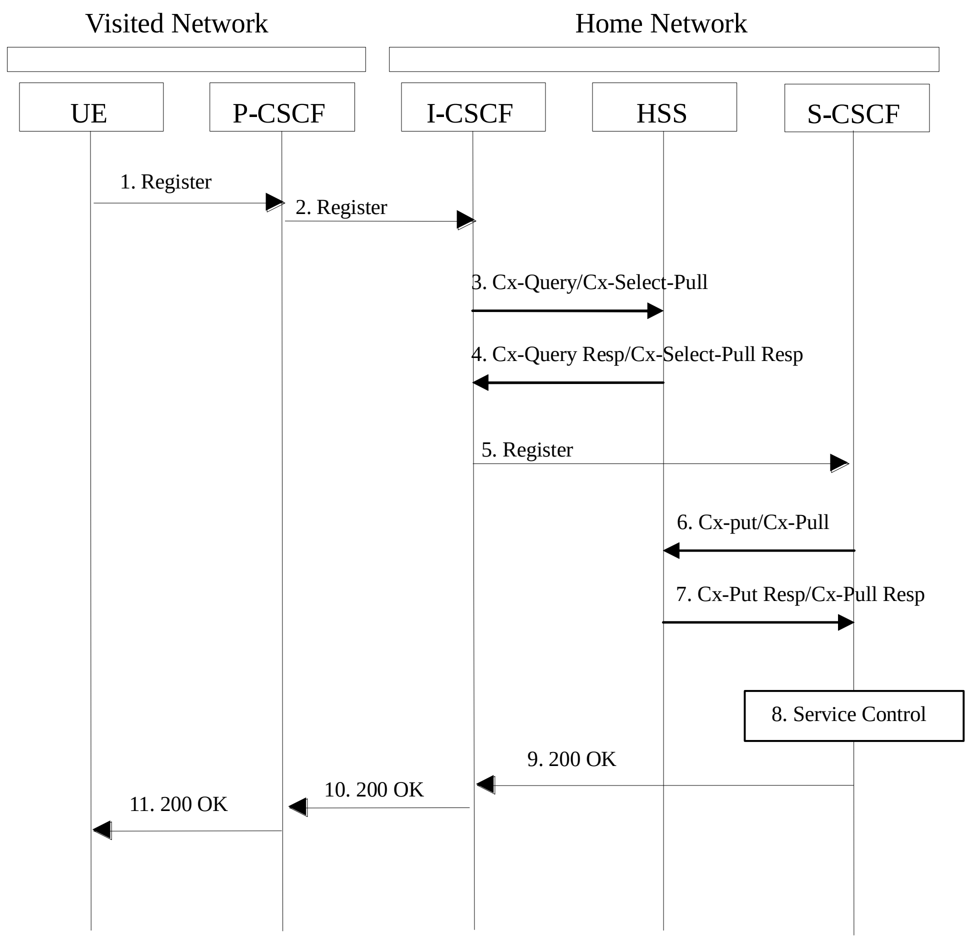

Figure 7.1: Registration – User not registered

1. After the UE has obtained IP connectivity, it can perform the IM registration. To do so, the UE sends the Register information flow to the proxy (Public User Identity, Private User Identity, home network domain name, UE IP address, Instance Identifier, GRUU Indication).

2. Upon receipt of the register information flow, the P-CSCF shall examine the "home domain name" to discover the entry point to the home network (i.e. the I-CSCF). The proxy shall send the Register information flow to the I-CSCF (P-CSCF address/name, Public User Identity, Private User Identity, P-CSCF network identifier, UE IP address). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. The P-CSCF network identifier is a string that identifies at the home

network, the network where the P-CSCF is located (e.g. the P-CSCF network identifier may be the domain name of the P-CSCF network).

3. The I-CSCF shall send the Cx-Query/Cx-Select-Pull information flow to the HSS (Public User Identity, Private User Identity, P-CSCF network identifier).

   The HSS shall check whether the user is registered already. The HSS shall indicate whether the user is allowed to register in that P-CSCF network (identified by the P-CSCF network identifier) according to the User subscription and operator limitations/restrictions if any.

4. Cx-Query Resp/Cx-Select-Pull Resp is sent from the HSS to the I-CSCF. It shall contain the S-CSCF name, if it is known by the HSS, or the S-CSCF capabilities, if it is necessary to select a new S-CSCF. When capabilities are returned the I-CSCF shall perform the new S-CSCF selection function based on the capabilities returned.

   If the checking in HSS was not successful the Cx-Query Resp shall reject the registration attempt.

5. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism. The I-CSCF also determines the name of a suitable home network contact point, possibly based on information received from the HSS. I-CSCF shall then send the register information flow (P-CSCF address/name, Public User Identity, Private User Identity, P-CSCF network identifier, UE IP address to the selected S-CSCF. The home network contact point will be used by the P-CSCF to forward session initiation signalling to the home network.

   The S-CSCF shall store the P-CSCF address/name, as supplied by the visited network. This represents the address/name that the home network forwards the subsequent terminating session signalling to the UE. The S-CSCF shall store the P-CSCF Network ID information.

6. The S-CSCF shall send Cx-Put/Cx-Pull (Public User Identity, Private User Identity, S-CSCF name) to the HSS.

7. The HSS shall store the S-CSCF name for that user and return the information flow Cx-Put Resp/Cx-Pull Resp (user information) to the S-CSCF. The user information passed from the HSS to the S-CSCF shall include one or more names/addresses information which can be used to access the platform(s) used for service control while the user is registered at this S-CSCF. The S-CSCF shall store the information for the indicated user. In addition to the names/addresses information, security information may also be sent for use within the S-CSCF.

8. Based on the filter criteria, the S-CSCF shall send register information to the service control platform and perform whatever service control procedures are appropriate.

9. The S-CSCF shall return the 200 OK information flow (home network contact information, a unique GRUU) to the I-CSCF.

10. The I-CSCF shall send information flow 200 OK (home network contact information, a unique GRUU) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

11. The P-CSCF shall store the home network contact information, and shall send information flow 200 OK (a unique GRUU) to the UE.

7.1.4 Re-Registration information flow – User currently registered

Periodic application level re-registration is initiated by the UE either to refresh an existing registration or in response to a change in the registration status of the UE. A re-registration procedure can also be initiated when the capabilities of the UE have changed. Re-registration follows the same process as defined in clause 7.1.3 "Registration Information Flow – User not registered". When initiated by the UE, based on the registration time established during the previous registration, the UE shall keep a timer shorter than the registration related timer in the network.

NOTE 1: If the UE does not re-register, any active sessions may be deactivated.

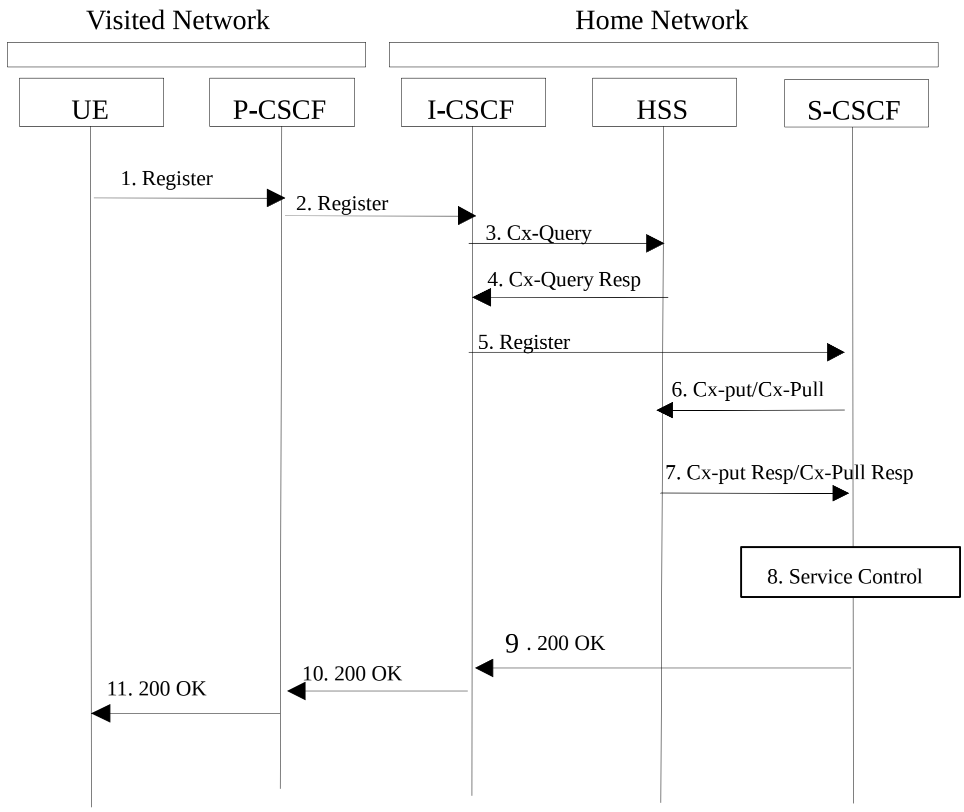

Figure 7.2: Re-registration - user currently registered

1. The UE initiates a re-registration. For periodic registration, the UE initiates a re-registration prior to expiry of the agreed registration timer. To re-register, the UE sends a new REGISTER request. The UE sends the REGISTER information flow to the proxy (Public User Identity, Private User Identity, home network domain name, UE IP address, capability information, Instance Identifier, GRUU Indication).

2. Upon receipt of the register information flow, the P-CSCF shall examine the "home domain name" to discover the entry point to the home network (i.e. the I-CSCF). The proxy does not use the entry point cached from prior registrations. The proxy shall send the Register information flow to the I-CSCF (P-CSCF address/name, Public User Identity, Private User Identity, P-CSCF network identifier, UE IP address). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. The P-CSCF network identifier is a string that identifies at the home network, the network where the P-CSCF is located (e.g., the P-CSCF network identifier may be the domain name of the P-CSCF network).

3. The I-CSCF shall send the Cx-Query information flow to the HSS (Public User Identity, Private User Identity and P-CSCF network identifier).

4. The HSS shall check whether the user is registered already and return an indication indicating that an S-CSCF is assigned. The Cx-Query Resp (indication of entry contact point, e.g. S-CSCF) is sent from the HSS to the I-CSCF.

5. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism. The I-CSCF also determines the name of a suitable home network contact point, possibly based on information received from the HSS. I-CSCF shall then send the register information flow (P-CSCF address/name, Public User Identity, Private User Identity, P-CSCF network identifier, UE IP address to the selected S-CSCF. The home network contact point will be used by the P-CSCF to forward session initiation signalling to the home network.

   The S-CSCF shall store the P-CSCF address/name, as supplied by the visited network. This represents the address/name that the home network forwards the subsequent terminating session signalling to the UE.

6. The S-CSCF shall send Cx-Put/Cx-Pull (Public User Identity, Private User Identity, S-CSCF name) to the HSS.

NOTE: Optionally as an optimisation, the S CSCF can detect that this is a re-registration and omit the Cx-Put/Cx-Pull request.

7. The HSS shall stores the S-CSCF name for that user and return the information flow Cx-Put Resp/Cx-Pull-Resp (user information) to the S-CSCF. The S-CSCF shall store the user information for that indicated user.

8. Based on the filter criteria, the S-CSCF shall send re-registration information to the service control platform and perform whatever service control procedures are appropriate.

9. The S-CSCF shall return the 200 OK information flow (home network contact information, a unique GRUU) to the I-CSCF.

10. The I-CSCF shall send information flow 200 OK (home network contact information, a unique GRUU) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

11. The P-CSCF shall store the home network contact information, and shall send information flow 200 OK (a unique GRUU) to the UE.

7.1.5 Stored information

Table 7.1 provides an indication of some of the information stored in the indicated nodes during and after the registration process.

NOTE: Table 7.1 is not an exhaustive list of stored information, i.e. there can be additional information stored due to registration.

Table 7.1: Information Storage before, during and after the registration process

Node	Before Registration	During Registration	After Registration
UE - in local network	Credentials Home Domain Proxy Name/Address	Same as before registration	Credentials Home Domain Proxy Name/Address
Proxy CSCF - in Home or Visited network	Routing Function	Initial Network Entry point UE Address Public and Private User IDs	Final Network Entry point UE Address Public and Private User IDs
Interrogating CSCF - in Home network	HSS or SLF Address	Serving CSCF address/name P CSCF Network ID Home Network contact Information	No State Information
HSS	User Service Profile	P CSCF Network ID	Serving CSCF address/name
Serving CSCF (Home)	No state information	HSS Address/name User profile (limited – as per network scenario) Proxy address/name P CSCF Network ID Public/Private User ID UE IP Address UE GRUU	May have session state Information Same as during registration

7.2 Session flows

7.2.1 Session Transfer Procedures

7.2.1.0 General

This section gives information flows for the procedures for performing session transfers. This is presented in two steps: first a basic primitive that can be used by endpoints to cause a multi-media session to be transferred, and second the procedures by which this primitive can be used to implement some well-known session-transfer services.

7.2.1.1 Refer operation

The refer primitive is an information flow indicating a "Refer" operation, which includes a component element "Refer-To" and a component element "Referred-By". The end point receiving a referral may be UE#1 as shown in the example flow in figure 7.3 or it may be any other type of originating entity as defined in clause 5.4a. The referring endpoint may be either UE#2 as shown, an Application Server or a non-IMS network SIP client. The referred-to destination may be UE#F as shown in figure 7.3 or it may be any other type of terminating entity as defined in clause 5.4a. Only the scenario in which a call from the first UE is referred by a second UE to a third UE is shown.

An information flow illustrating this is as follows:

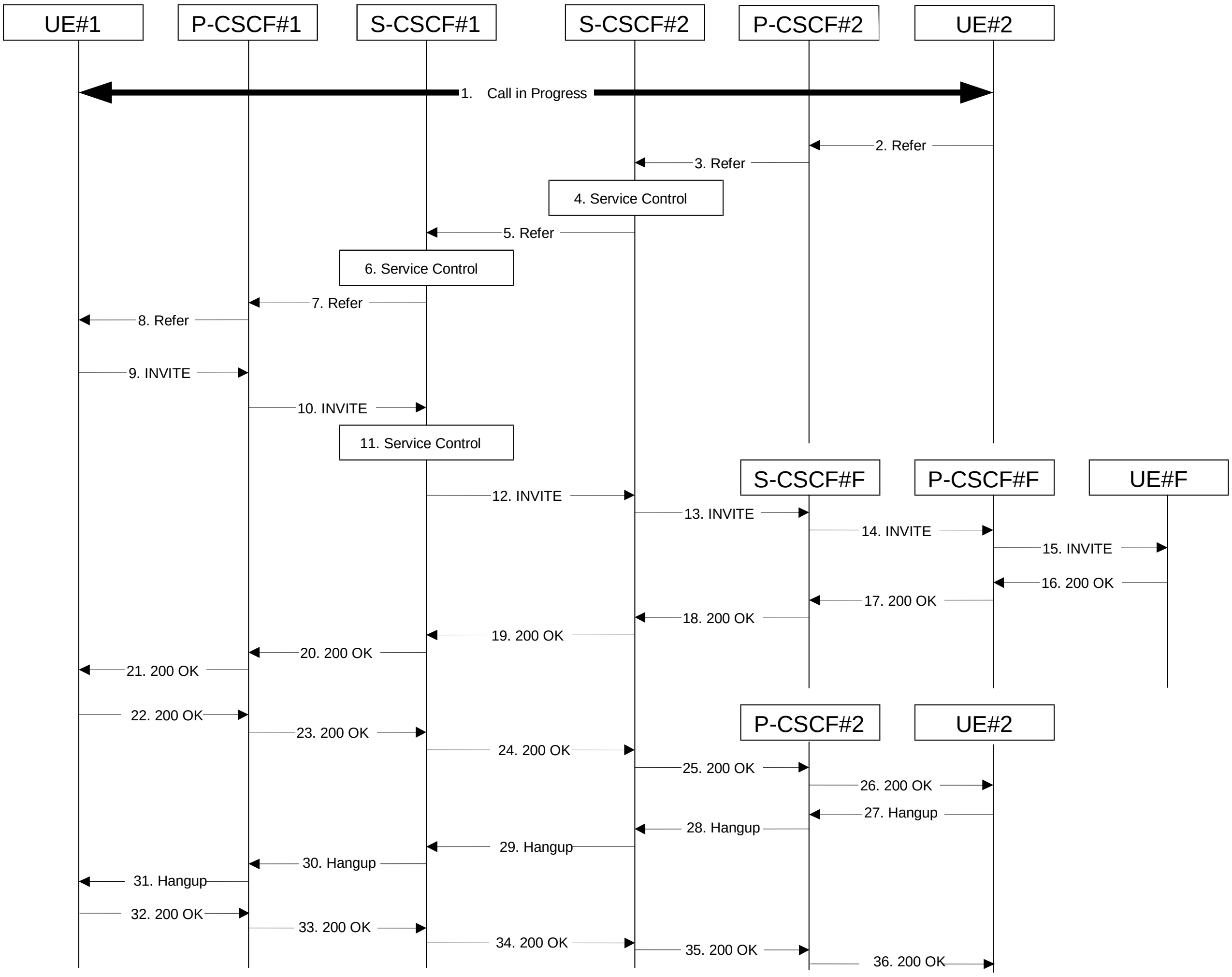

Figure 7.3: Refer operation

Step-by-step description of the information flow:

1. A multi-media session is assumed to already exist between UE#1 and UE#2, established either as a basic session or by one of the supplemental services described in this subclause.

2. UE#2 sends the Refer command to P-CSCF#2, containing "Refer-To" UE#F and "Referred-By" UE#2. If UE#2 knows the GRUU of UE#F the "Refer-To" contains the GRUU of UE#F otherwise the "Refer-To" contains the Public User Identity of UE#F.

3. P-CSCF#2 forwards the message to S-CSCF#2.

4. S-CSCF#2 invokes whatever service logic is appropriate for this request. If UE#2 does not subscribe to a transfer service, service logic may reject the request. If S-CSCF#2 service logic requires that it remain on the path for the subsequent request, the service logic generates a private URI, addressed to itself, the "Refer-To" value in the request with the private URI.

5. S-CSCF#2 forwards the message to S-CSCF#1.

6. S-CSCF#1 invokes whatever service logic is appropriate for this request. To hide the identities of UE#2 and UE#F, S-CSCF#1 service logic stores the "Refer-To" and "Referred-By" information and replaces them with private URIs.

7. S-CSCF#1 forwards the message to P-CSCF#1.

8. P-CSCF#1 forwards the message to UE#1.

9. UE#1 initiates a new multi-media session to the destination given by the "Refer-To", which may either be a URI for UE#F, a private URI pointing to S-CSCF#2, or a private URI pointing to S-CSCF#1.

10. P-CSCF#1 forwards the INVITE request to S-CSCF#1.

11. S-CSCF#1 retrieves the destination information for the new session, and invokes whatever service logic is appropriate for this new session.

12. S-CSCF#1 determines the network operator addressed by the destination URI, and forwards the INVITE to either S-CSCF#F or S-CSCF#2 (actually I-CSCF#F or I-CSCF#2, the public entry points for S-CSCF#F and S-CSCF#2, respectively). If S-CSCF#1 forwards the INVITE to S-CSCF#F, the procedure continues with step #14, bypassing step #13.

13. S-CSCF#2 decodes the private URI destination, and determines the final destination of the new session. It determines the network operator addressed by the destination URI. The request is then forwarded onward to S-CSCF#F as in a normal session establishment.

14. S-CSCF#F invokes whatever service logic is appropriate for this new session, and forwards the request to P-CSCF#F.

15. P-CSCF#F forwards the request to UE#F.

16-21. The normal session establishment continues through bearer establishment, optional alerting, and reaches the point when the new session is accepted by UE#F. UE#F then sends the 200-OK final response to P-CSCF#F, which is forwarded through S-CSCF#F, S-CSCF#2 (optionally), S-CSCF#1, P-CSCF#1, to UE#1. At this point a new session is successfully established between UE#1 and UE#F.

22-26. The Refer request was successful, and UE#1 sends a 200-OK final response to UE#2. This response is sent through P-CSCF#1, S-CSCF#1, S-CSCF#2, P-CSCF#2, and to UE#2.

27-31. UE#2 clears the original session with UE#1 by sending the BYE message. This message is routed through P-CSCF#2, S-CSCF#2, S-CSCF#1, P-CSCF#1, to UE#1.

32-36. UE#1 acknowledges the BYE and terminates the original session. It responds with the 200-OK response, routed through P-CSCF#1, S-CSCF#1, S-CSCF#2, P-CSCF#2, to UE#2.

NOTE: The last BYE message to clear the original session can be issued either by UE#1 or by UE#2.

Annex A (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2005-11	SA2#49	-	-	-	Skeleton (S2-052781)	-	0.0.1
2005-11	SA2#49	-	-	-	Output from TSG SA2 #49 taking into account: S2-052983; S2-052752; S2-052984; S2-052985; S2-053048	0.0.1	0.1.0
2006-03	SA2#51	-	-	-	Output from TSG SA2 #51 taking into account: S2-060771; S2-061134; S2-061135; S2-061136; S2-061212	0.2.1	0.3.0
2006-04	SA2#52	-	-	-	Update Editors notes to be correct style	0.3.0	0.3.1
2006-05	SA2#52	-	-	-	Output from TSG SA2 #52 taking into account: S2-061516; S2-061686; S2-061788; S2-061962; S2-061791; S2-061792; S2-061790 To be sent to TSG SA for Information	0.3.1	1.0.0
2006-05	SA#32	SP-060295	-	-	MCC Editorial Update for presentation to TSG SA#32 for information (clauses 5.2.2.x and 5.11.6.y renumbered to 7.1.x and 7.2.1.y).	1.0.0	1.0.1