**3GPP TSG CT Meeting #28** **CP-050052**
**1st – 3rd June 2005. Quebec, CANADA.**

**Source:** **CT1**

**Title:** **Liaison statements sent from CT1 since TSG#27**

**Agenda item:** **6.1.1**

**Document for:** **INFORMATION**

This document contains following liaison statements that have been sent by CT1 since TSG#27:

| TDoc # | Tdoc Title | To: |
|---|---|---|
| C1-050659 | Reponse to Reply LS on Application Charging ID (ACID) for PoC | To: SA5;CC: SA2 |
| C1-050666 | Reply to Reply LS on protocol aspects for CSI | To: SA2 |
| C1-050677 | LS on Identifying and charging for multiple session branches generated by a UAC or proxy | To: SA5 |
| C1-050728 | LS on Inclusion of I-WLAN as a valid access technology to IMS | To: SA2; CC: CT |
| C1-050796 | Reply to LS on service based inter-system hand over | To: GERAN2; CC: SA1, SA2, CT3 |
| C1-050797 | LS on NAS actions in support of MBMS Reception | To: RAN2, SA2, GERAN2; CC: RAN3, CT4, SA1 |
| C1-050798 | Reply to LS on optional support of DSAC and Network sharing in Rel-5 Ues | To: SA, RAN2; CC: RAN, CT |
| C1-050799 | Reply to LS on GPRS P-CSCF discovery procedure | To: SA2; CC: CT3 |
| C1-050805 | LS to TSG CT and RAN on CSI interoperability testing (related to WID in C1-050462) | To: CT; RAN; CC: SA |
| C1-050806 | Response to LS from SA3 on misalignment between TS 33.220 and TS 24.109 | To: SA3 |

# 3GPP TSG-CT1 Meeting #38 Tdoc C1-050623
# Cancun, Mexico, 25-29 April 2005

**Source:** Lucent Technologies

**Title:** Identifying and charging for multiple session branches generated by a UAC or proxy

**Agenda item:** 6.2

**Document for:** DISCUSSION

## Problem Statement

Current procedures allow for various UACs and proxies in the IMS under certain circumstances to generate multiple outgoing branches (e.g., INVITE transactions) for a single incoming event (e.g., incoming IAM at an MGCF or incoming INVITE request at a proxy). There are three possible reasons this may occur: *retry on error, forking and recursion (redirection)*.

TS 24.229 indicates that in some cases, all branches are assigned the same ICID for charging purposes. TS 24.229 leaves other cases unspecified. As a result, when multiple branches occur during a session, the charging system will typically receive charging records from the various IMS nodes associated with the different branches of the request, all with the same ICID. *There is insufficient information to uniquely identify which records are associated with which branch, or to determine the sequence in which the branches were created*. Note that the term-ioi may also differ across the branches.

As a result, it is generally only possible to charge the final success branch, even when, for example, the final node on a preceding branch causes a redirection to a different user by sending a 3xx response. So it is *not possible to uniquely identify and charge the redirecting party*. It is also unclear how the charging system should combine charging information from multiple branches. The branch result and called party information may differ from branch to branch.

## Use Cases

### Recursion (Redirection)

As a standard feature of RFC 3261, any proxy or UA in the IMS may receive a 3xx response and may recurse on the response to create a new branch for a request in a manner similar to retry on error and forking. In particular, the MGCF in Release 6 may do so. The AS from Release 5 onward may also recurse. Proxies are not precluded from doing so in Release 5 onward. As proposed in a previous discussion document, it may be appropriate to *limit recursion to the MGCF, AS, I-CSCF and BGCF*. (The UE may always do so but does not create charging records.)

In all cases, the charging records from the redirecting branch (that returns a 3xx response) will have the same ICID as charging records from subsequent branches. Charging records from the redirecting branch will be success event records (3xx redirection is defined as successful from a charging perspective). If multiple success branches occur due to redirection, there is *insufficient information to uniquely determine the branch that provided the contact information for recursion*, although it may be possible to distinguish between charging records for different redirecting branches by the called party information used on each branch.

This is not acceptable from a charging perspective since the parent branches must be known to determine if a request was redirected and who redirected it, especially when recursion occurs in combination with retry and/or forking. *It is not always possible to charge the redirecting party when redirection occurs*.

### Forwarding

An AS in Release 5 onwards may change the target of a request (i.e., forward the request). This is not a form of branching but is worth noting due to its similarity to redirection. Forwarding is essentially redirection without a separate redirecting branch. Another way of putting it is that the AS, on behalf of the registered user, causes itself to recurse on the target without even making the first branch attempt. The charging procedures for recursion and forwarding should be identical for the redirected/forwarded branch.

### Serial Forking

The S-CSCF in Release 6 may perform forking on a SIP request to a public user identity registered to multiple private user identities.  An AS in Release 5 onwards may also perform serial forking.

In either case, the charging records from all branches will have the same ICID and there is insufficient information to determine the sequence of branches.  It may also be difficult to distinguish between different branches that terminate with the same error.

This may be acceptable from a charging perspective if it is clear that there are no charging implications associated with the failure branches and it is acceptable to discard charging information from the failure branches.  *Is it important to know which branches fail when forking*?  For example, is important to document that higher priority targets were attempted and failed before lower priority targets are tried, given that the lower priority targets may involve additional charges (e.g., roaming)?

### Parallel Forking

For Release 6, the discussion of serial forking also applies to parallel forking, except that the branches are not sequenced.  In addition, more than one branch may succeed with 200 OK (INVITE).  Although all but one of these will be cleared by the UAC, *current charging procedures will create separate charging start records for each successful branch*.  The charging system may not be able to distinguish between charging records created by nodes on different branches.

### Retry on Error

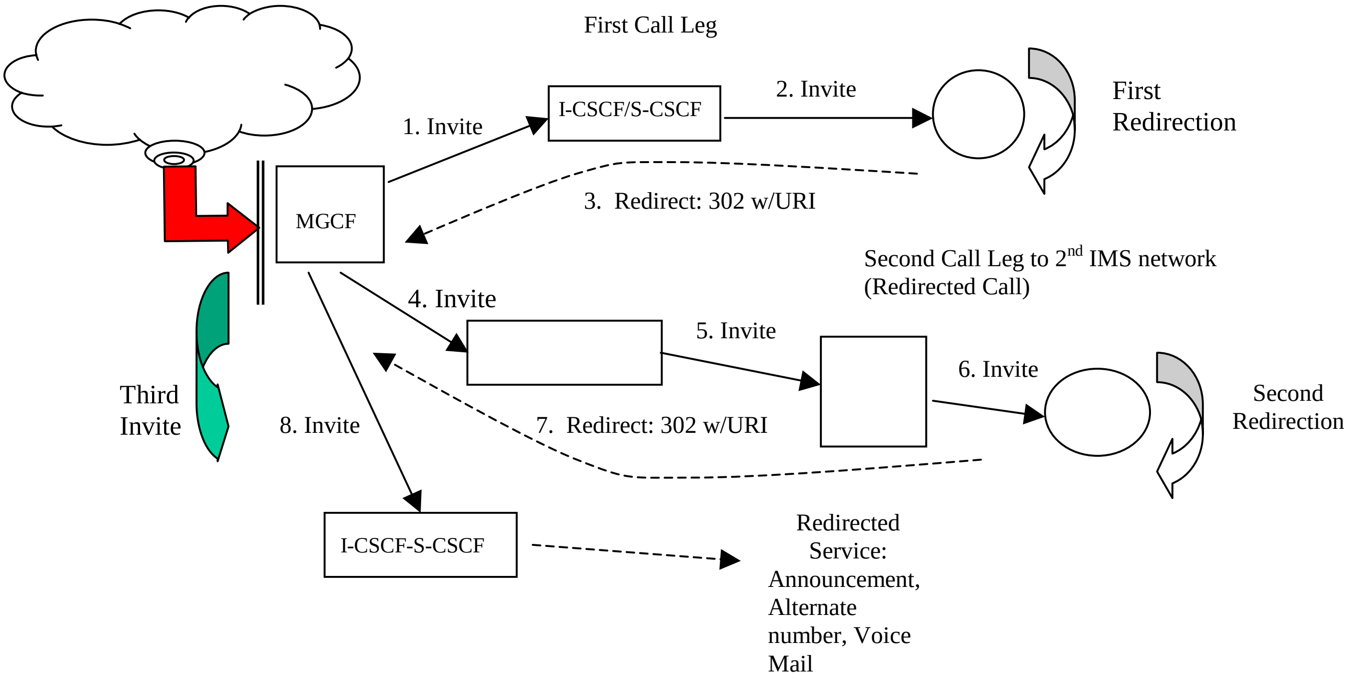
This case only applies to UACs in the IMS that participate in the charging architecture – MGCF and AS (as UA).

For example, if the first branch of an INVITE request from an outgoing MGCF fails with a 420 or other recoverable error, the MGCF may retry if it is able to modify the request so as to eliminate the reason for the initial error.  TS 24.229 implies that the SIP requests from the first error and subsequent branches will have the same ICID.  Charging records from the first branch will be error event records, but if multiple branches occur there is insufficient information to determine the sequence of branches or to distinguish between different branches with the same error.

This may be acceptable from a charging perspective if it is clear that there are no charging implications associated with the failure branches and it is acceptable to discard charging information from the failure branches.  *Is it important to know which branches fail due to potentially correctable errors*?  For example, if certain endpoints always fail the first attempt due to lack of a software upgrade, either additional unnecessary signalling will occur before successful session establishment, the UAC will attempt other (potentially more expensive) targets, or the request will fail.  It may be useful to have access to this failure history information to properly manage and charge for the use of the network resources.

## Example Flow 1

This example shows a multiple leg redirection scenario to demonstrate the charging implications of the current procedures.



In this example, when the outgoing MGCF receives an IAM from the PSTN, it sends an INVITE request to an I-CSCF for its domain (step1). The 1st called party has a redirecting service enabled within an AS (step 3). When the MGCF receives the redirection response, it may choose to recurse or fail the call. If it chooses to recurse, it sends an INVITE request to the URI in the contact header of the response, where the URI is associated with a 2nd IMS network (step 4), thus creating a 2nd branch of the original request to the 2nd called party. This request is routed through an AS to the 2nd called party's UE, which chooses to redirect the request to a 3rd called party (step 7). The MGCF chooses to recurse again and sends an INVITE request to the 3rd call party identified in the contact header of the 2nd redirection (step 8). The charging system will receive success charging event records from nodes on the first two branches of the request and other charging records from the final branch, all with the same ICID. The charging system cannot reconstruct the sequence in which nodes are visited due to the lack of sequencing information in the charging records and the coarse granularity of the time stamps. Thus it is not possible to identify the party invoking the redirection to the 3rd called party to apply the desired charging discipline.

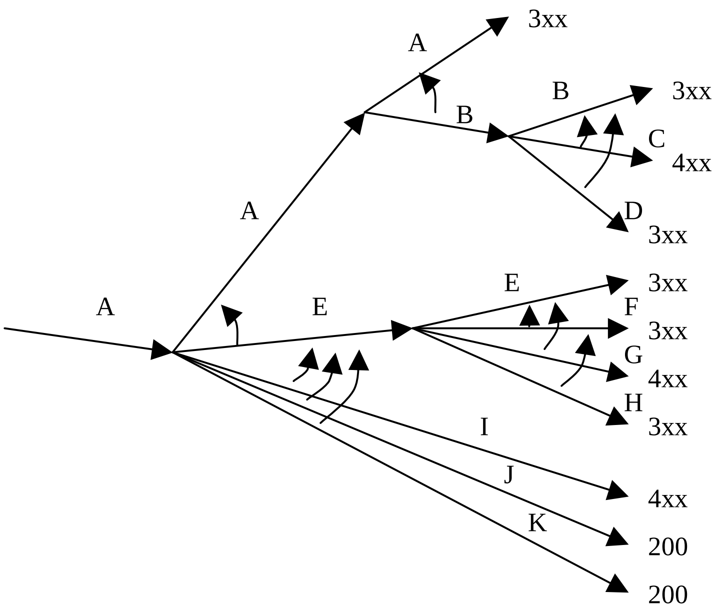
The minimum information required to reconstruct the necessary charging information is:

- For each branch, list all the nodes creating charging records for the branch, the called party (Request URI) on the branch, and the final outcome (2xx-6xx) of the branch.
- For each branch, identify the branch (current or previous) that provides the called party (Request URI) for the branch.

Other examples might show the use of redirection in combination with retry and forking, or show recursion at an AS or I-CSCF, but the charging principles are identical.

## Example Flow 2

The following figure is a more theoretical example of a complex combination of branches due to redirection, retry on error, serial forking and parallel forking, which demonstrates many of the issues that can arise for charging. Branches are shown in numbered sequence. Antecedent branches are identified by both curves in the figure and the text descriptions of the sequence shown to the right of the figure. It would be appropriate to test any solution against a more elaborate example like this one to validate the ability of the charging architecture to identify the correct users to be charge.



1. A redirects A to B

2. B redirects B to C or D

3. Fork C fails

4. Fork D redirects D to E

5. E redirects E to F or G

6. Fork F redirects F to H

7. Fork G fails

8. Fork H redirects H to I and K

9. I fails

10. I retried as J and succeeds

11. K succeeds

## Inconsistencies in 3xx handling

The Release 5 charging specification TS 32.225 has an inconsistency in 3xx handling that has been propagated to Release 6 documents TS 32.260, TS 32.296 and TS 32.298. Clause 5.2.4.37 of TS 32.225, Service Delivery Start Time Stamp, states that 3xx is an unsuccessful case, while clause 7.2.9, Cause-Code AVP, indicates that 3xx is a successful case. SA5 has discussed this issue and seems to prefer to identify 3xx as a successful case. CRs are expected soon to resolve this discrepancy, but there are still problems. The result code (3xx) is not stored in the charging record, so *we cannot distinguish between the different types of redirect (e.g., 302 and 305*), which have very different semantics. Furthermore, it is not clear how to determine whether or not this successful event causes a node to recurse without knowing the precise antecedent branch.

For atomic requests, this charging strategy is also faulty since there is *no way to distinguish between a normal success event and a redirect success event for an atomic request such as METHOD*.

Regardless of how these problems are resolved, we assume that the charging record in the case of redirection must include the result code or equivalent information to distinguish among the different “success” cases. We expect to take in the appropriate CRs to SA5 to resolve this issue.

## Solution Requirements

The key requirement to enable proper charging for recursion is to clearly identify the antecedent branch (which provides the new called party) for each branch. It is not sufficient to uniquely identify each branch since time sequence information is lost due to the coarse granularity of the time stamp. Even if it is possible to reconstruct the exact sequence of branches, there is insufficient information to uniquely identify each antecedent branch.

Due to the complexities associated with correctly associating charging records with each branch, and the desire to provide procedures that are as robust as possible when future feature are adopted that impact the branching process, it seems appropriate to create a unique identifier for every branch. If there are no charging implications to certain failed branches, then the corresponding records can be easily identified and discarded. If there are charging implications to these failed branches, now or in the future, they can be easily identified.

*Every branch associated with a single request should have*

- *a unique identifier common to all nodes in the branch and*
- *a parameter identifying its antecedent branch, if one exists*.

Note that the first branch never has an antecedent but all others do.

**Unique branch identifier**

The most straightforward way to satisfy the first solution requirement is for a node to assign a new ICID every time it creates a new branch.  Just adding a branch number to the ICID could accomplish this, although this would have to be done in such a way that the branch identifiers remain unique even when different entities branch on the same request.  A possible alternative is to add a unique branch identifier from the existing SIP messages to each charging record.

**Uniquely identifying the antecedent branch**

If a new ICID is assigned to each new branch, then the charging record could identify the antecedent branch by including a new parameter whose value is the ICID of the antecedent branch.  Let's call this new parameter a Linked ICID (L-ICID).

## Proposal

SA5 has recently discussed this issue but has made no decision yet on how to proceed.

We believe that the problems with charging for branches as discussed in this document require essential corrections to Release 5 and Release 6 since it is not always possible with the current procedures to charge the correct user for IMS services when redirection is employed.

*We propose to generate an outgoing liaison from CT1 to SA5 with the following content:*

- CT1 has examined cases of SIP branching due to redirection, forking and retry on error and has concluded that it is not always possible with existing procedures to charge the correct party when an IMS node recurses on a 3xx redirection response.  CT1 believes this problem to require an essential correction to procedures in Release 5 and Release 6.
- CT1 believes that a potential solution to the problem contains the following elements:
    - Each branch of a request must be assigned unique identifying information for charging purposes (potentially a different ICID).
    - Charging records must include information identifying the antecedent branch when a node recurses on a redirection response.
    - Charging records for a redirecting branch must include information identifying the type of redirection (e.g., 302 or 305) to distinguish between the types of redirection and to distinguish it from the 200 OK success case.
- Further information can be found in this contribution.
- CT1 wishes to inform SA5 that procedures in TS 24.229 are only intended to describe when to include an ICID within a SIP message.  CT1 understands that specifications under control of SA5 are to describe how to assign values to an ICID.  CT1 furthermore has no control over the content of charging records.
- CT1 respectfully requests SA5 to examine this information, make any necessary corrections to specifications under its control, and to inform CT1 and any other affected groups if other changes are needed.

# 3GPP TSG-CT1 Meeting #38 Tdoc C1-050659
# Cancun, Mexico, 25-29 April 2005

| | |
|---|---|
| **Title:** | Reply LS on Application Charging ID (ACID) for PoC |
| **Response to:** | LS (S5-054289/C1-050437) on Reply LS on Application Charging ID (ACID) for PoC from SA5 |
| **Release:** | Rel-6 |
| **Work Item:** | |
| **Source:** | CT1 |
| **To:** | SA5 |
| **Cc:** | SA2 |

**Contact Person:**

| | |
|---|---|
| **Name:** | Keith Drage |
| **Tel. Number:** | +44 1793 776249 |
| **E-mail Address:** | drage@lucent.com |

**Attachments:** None

---

### 1. Overall Description:

CT1 thanks their SA5 for their liaison statement on Application Charging ID (ACID).

CT1 understands that the proposal is made primarily for the support of PoC phase 1 in OMA, from your statement in the incoming liaison statement:

> "In SA5, the ACID is currently only being specified for the PoC service as detailed in the request from OMA PoC WG (attached for convenience). From SA5 perspective, the attachment contains all the information needed to specify this "PoC-only" Application ID".

It is however of the understanding of experts in CT1 that the current PoC phase 1 specifications do not need such a capability, although it may be needed for PoC phase 2. Therefore such support would appear to be currently unnecessary in 3GPP release 6.

CT1 would further note that any inclusion of a new P-Charging-Vector parameter needs documentation in 3GPP TS 24.229 and as such cannot be documented in a PoC specific manner, but must be treated in a generic manner by all IMS entities other than the Application Server providing the PoC functionality. Even at the application server, the header must be extracted in 3GPP 24.229 procedures, before usage by the application itself. CT1 currently has insufficient material from SA5 to perform this specification work in 3GPP TS 24.229.

### 2. Actions:

**To SA5 group.**

**ACTION:** CT1 asks SA5 group to . . . .

Investigate whether such a capability is still required in release 6, or whether it should be deferred until work starts on support of later PoC capabilities.

If the capability is required in release 6, then provide sufficient information to CT1 to allow specification of the necessary changes to 3GPP TS 24.229.

If the capability is required in release 6, then provide sufficient information to SA plenary to allow an exception to be identified to release 6 completion on behalf of CT1.

### 3. Date of Next TSG-CN1 Meetings:

| | | |
|---|---|---|
| CT1_38 | 25th -29th April 2005 | Cancun, Mexico |
| CT1_39 | 29th August – 2nd September 2005 | London, UK |

# 3GPP TSG-CT1 Meeting #38 Tdoc C1-050666
# Cancun, Mexico, 25-29 April 2005

|  |  |
|---|---|
| **Title:** | Reply LS to CT1 on protocol aspects for CSI |
| **Response to:** | LS (S2-050954/C1-050588) on Reply LS to CT1 on protocol aspects for CSI from SA2 |
| **Release:** | Rel-6 |
| **Work Item:** | CSICS |
| **Source:** | CT1 |
| **To:** | SA2 |
| **Cc:** |  |

**Contact Person:**

|  |  |
|---|---|
| **Name:** | Atle Monrad |
| **Tel. Number:** | +47 454 10 665 |
| **E-mail Address:** | atle.monrad@ericsson.com |

**Attachments:** None

---

**1. Overall Description:**

CT1 would like to thank SA2 for their LS S2-**050954** on protocol aspects for CSI and the description of the current CSI architecture outlined in TS 23.279.

CT1 has discussed both the technical architecture and also the question in the Editor's Note outlined in the LS S2-050954. Some concerns have been raised with regards to the capability exchange mechanism. CT1 therefore, kindly request the clarifications outlined below.

**2. Actions:**

**To SA2 group.**

CT1 would like to answer SA2's questions from a CT1 perspective:

For the following Editor's Note:

*It shall be possible for a UE to request the OPTIONS request to be sent to any other registered UE. E.g. in case there is an ongoing CS call between UE-A and UE-B, the requirement would make it possible for UE-A to retrieve the UE capability information from UE-B.*

*Editor's Note: The feasibility from a stage 3 perspective of the requirement above paragraph needs to be evaluated by 3GPP CT1*

CT1 sees problems in the usage of the OPTIONS request, especially when it comes to forking of the OPTIONS requests. Also it was indicated by IETF that the OPTIONS request shall not be used to transfer capabilities of a UE, only the OPTIONS 200 (OK) response is used for capability transfer. It was also discussed whether the OPTIONS request in IMS will only be used for the CSI capabilities exchange or also for other capabilities/services. Therefore CT1 requests SA2 to give more guidance on the functional requirements for the capability exchange for CSI, so that CT1 can discuss and work on a technical solution.

CT1 also requests a response to the following issue:

CT1 discussed a possible problem if the Tel-URI that a user has in their IMS subscription is different from the MSISDN for the user's CS subscription. If such a case exists, then the SIP routing of an OPTIONS request with an MSISDN from one UE to the other cannot be guaranteed.

**ACTION:**

CT1 kindly asks SA2 to take the above issues into account when discussing CSI and also to provide feedback on the questions from CT1. CT1 also asks to be kept updated with any information resulting from further SA2 investigations related to CSI.

**3. Date of Next TSG-CN1 Meetings:**

| | | |
|---|---|---|
| CT1_39 | 29th August – 2nd September 2005 | London, UK |

**3GPP TSG-CT1 Meeting #38** **Tdoc ⌘C1-050673**
**Cancun, Mexico, April 25th – April 29th, 2005**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.229** | **CR** | **869** | ⌘**rev** | **1** | ⌘ | Current version: | **5.12.0** | ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Port 5060 | | |
| ***Source:*** | ⌘ | Ericsson | | |
| ***Work item code:*** | ⌘ | IMS-CCR | ***Date:*** ⌘ | 12/04/2005 |
| ***Category:*** | ⌘ | F | ***Release:*** ⌘ | Rel-5 |
| | | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | *Use one of the following releases:* | *Ph2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)*<br>*Rel-7 (Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | RFC 3261 recommends, but not mandate, the port 5060 to be used for initial SIP communication.<br>It is proposed to clearly specify that the UE should use port 5060 in case no other initial port number is given and to clearly specify that the P-CSCF must listen to at least port 5060. |
| ***Summary of change:*** | ⌘ | Clearly specify that the well known port 5060 (recommended by RFC 3261) is used in IMS as the default port in case no port information is available in the UE |
| ***Consequences if not approved:*** | ⌘ | No default port is specified for IMS, leading to that SIP registration and consequently all SIP communication can fail. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 4.2A, 5.1.1.2, 5.2.2 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs Affected:*** | ⌘ | | X | Other core specifications | ⌘ | |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** First change *****

## 4.2A Transport mechanisms

This document makes no requirement on the transport protocol used to transfer signalling information over and above that specified in RFC 3261 [26] clause 18. However, the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] subclause 18.1.1, even if a mechanism exists of discovering a maximum transmission unit size longer than 1500 bytes.

For initial REGISTER requests, the UE and the P-CSCF shall apply port handling according to subclause 5.1.1.2 and subclause 5.2.2.

The UE and the P-CSCF shall send and receive request and responses other then initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [19].

***** Second change *****

### 5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

The UE shall send only the initial REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261 [26].

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the Authorization header, with the username field, set to the value of the private user identity;

b) the From header set to the SIP URI that contains the public user identity to be registered;

c) the To header set to the SIP URI that contains the public user identity to be registered;

d) the Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) the Via header containing the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field.

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) the Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

i) the Supported header containing the option tag "path"; and

j) if a security association exists, a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;

e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and

f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

***** Third change *****

### 5.2.2 Registration

The P-CSCF shall be prepared to receive only the initial REGISTER requests on the SIP default port values as specified in RFC 3261 [26]. The P-CSCF shall also be prepared to receive the initial REGISTER requests on the port advertised to the UE during the P-CSCF discovery procedure.

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

1) insert a Path header in the request including an entry containing:

- the SIP URI identifying the P-CSCF;

- an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

2) insert a Require header containing the option tag "path";

3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'sec-agree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

   a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;

   b) if the security association the REGISTER request was received on, is an already established one, then:

      - the P-CSCF shall remove the Security-Verify header if it is present, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;

      - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;

      - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and

   c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

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

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

2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;

4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and

RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

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

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

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

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

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

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

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

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

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

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

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

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

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

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

1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;

2) keep the newly established set of security associations created during this authentication;

3) delete, if existing, any other set of security associations towards this UE immediately; and,

4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

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

1) keep the newly established set of security associations created during this authentication;

2) delete, if existing, any other set of security associations towards this UE immediately; and,

3) use the kept newly established set of security associations for further messages sent towards the UE.

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

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

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

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

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

**3GPP TSG-CT1 Meeting #38**
**Cancun, Mexico, April 25th – April 29th, 2005**

**Tdoc ⌘C1-050674**

CR-Form-v7.1

# CHANGE REQUEST

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.229** | **CR** | **871** | ⌘**rev** | **1** | ⌘ | Current version: | **6.6.0** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Port for 5060 | | |
| ***Source:*** | ⌘ | Ericsson | | |
| ***Work item code:*** | ⌘ | IMS-CCR | ***Date:*** ⌘ | 15/03/2005 |
| ***Category:*** | ⌘ | **A** | ***Release:*** ⌘ | Rel-6 |

*Use one of the following categories:*
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | RFC 3261 recommends, but not mandate, the port 5060 to be used for initial SIP communication.<br>It is proposed to clearly specify that the UE should use port 5060 in case no other initial port number is given and to clearly specify that the P-CSCF must listen to at least port 5060. |
| ***Summary of change:*** | ⌘ | Clearly specify that the well known port 5060 (recommended by RFC 3261) is used in IMS as the default port in case no port information is available in the UE |
| ***Consequences if not approved:*** | ⌘ | No default port is specified for IMS, leading to that SIP registration and consequently all SIP communication can fail. |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.1.1.2, 5.2.2 | | | |
| | | **Y** | **N** | | |
| ***Other specs affected:*** | ⌘ | | X | Other core specifications | ⌘ |
| | | | X | Test specifications | |
| | | | X | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | | |

**How to create CRs using this form:**

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks"  feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text.  Delete those parts of the specification which are not relevant to the change request.

***** First change *****

# 4.2A Transport mechanisms

This document makes no requirement on the transport protocol used to transfer signalling information over and above that specified in RFC 3261 [26] clause 18. However, the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] subclause 18.1.1, even if a mechanism exists of discovering a maximum transmission unit size longer than 1500 bytes.

For initial REGISTER requests, the UE and the P-CSCF shall apply port handling according to subclause 5.1.1.2 and subclause 5.2.2.

The UE and the P-CSCF shall send and receive request and responses other then initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [19].

***** Second change *****

### 5.1.1.2 Initial registration

The UE can register a public user identity with its contact address at any time after it has aquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

The UE shall send only the initial REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261 [26].

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field, set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

i) the Supported header containing the option tag "path"; and

j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;

e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

***** Third change *****

## 5.2.2 Registration

The P-CSCF shall be prepared to receive only the initial REGISTER requests on the SIP default port values as specified in RFC 3261 [26]. The P-CSCF shall also be prepared to receive the initial REGISTER requests on the port advertised to the UE during the P-CSCF discovery procedure.

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

1) insert a Path header in the request including an entry containing:

   - the SIP URI identifying the P-CSCF;

   - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

2) insert a Require header containing the option tag "path";

3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

    a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header;

    b) if the security association the REGISTER request was received on, is an already established one, then:

        - the P-CSCF shall remove the Security-Verify header if it is present;

        - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;

        - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and

    c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

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

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

2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;

4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

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

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

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

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

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

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

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

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

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

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

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

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

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

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

1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;

2) keep the newly established set of security associations created during this authentication;

3) delete, if existing, any other set of security associations towards this UE immediately; and

4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

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

1) keep the newly established set of security associations created during this authentication;

2) delete, if existing, any other set of security associations towards this UE immediately; and

3) use the kept newly established set of security associations for further messages sent towards the UE.

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

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

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

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

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

**3GPP TSG-CT1 Meeting #38 Tdoc C1-050677**
**Cancun, Mexico, 25-29 April 2005**

| | |
|---|---|
| **Title:** | LS on Identifying and charging for multiple session branches generated by a UAC or proxy |
| **Release:** | Release 5 / Release 6 |
| **Work Item:** | IMS-CCR |
| | |
| **Source:** | CT1 |
| **To:** | SA5 |
| **Cc:** | --- |

**Contact Person:**

| | |
|---|---|
| **Name:** | Keith Drage |
| **Tel. Number:** | +44 1793 776249 |
| **E-mail Address:** | drage@lucent.com |

| | |
|---|---|
| **Attachments:** | C1-050623 |

## 1. Overall Description:

CT1 has examined cases of SIP branching due to redirection, forking and retry on error (as identified in the attached contribution) and has concluded that problems with existing procedures to charge the correct party when an IMS node recurses on a 3xx redirection response may occur.

CT1 has identified cases where branching may require additional information to distinguish the different CDRs generated by different branches within such calls.

For redirection and retry on error, there are no differences between release 5 and release 6, so any changes assumed essential for release 6 could also be assumed to be essential for release 5. Forking is introduced in release 6.

CT1 wishes to inform SA5 that procedures in TS 24.229 are only intended to describe when to include an ICID within a SIP message. CT1 understands that specifications under control of SA5 are to describe how to assign values to an ICID. CT1 furthermore has no control over the content of charging records.

CT1 therefore believes that the first investigation of this issue needs to be performed by SA5 as they hold responsibility for identifying the charging needs (i.e. working the stage 1 and stage 2 issues). CT1 will provide any appropriate corrections in response to the SA5 investigations if needed.

## 2. Actions:

**To SA5 group.**

**ACTION:**

CT1 respectfully requests SA5 to examine this information, if needed make any necessary corrections to specifications under its control, and to inform CT1 and any other affected groups if other changes are needed.

## 3. Date of Next TSG-CN1 Meetings:

| | | |
|---|---|---|
| CT1_39 | 29th August – 2nd September 2005 | London, UK |

# 3GPP TSG-CT1 Meeting #38 Tdoc C1-050728
# Cancun, Mexico, 25-29 April 2005

| | |
|---|---|
| **Title:** | I-WLAN as access technology for IMS |
| **Response to:** | - |
| **Release:** | Rel-6 |
| **Work Item:** | IMS2 / WLAN |
| | |
| **Source:** | CT1 |
| **To:** | SA2 |
| **Cc:** | CT |

**Contact Person:**

| | |
|---|---|
| **Name:** | Atle Monrad |
| **Tel. Number:** | +47 454 10 665 |
| **E-mail Address:** | atle.monrad@ericsson.com |

**Attachments:** C1-050729

### 1. Overall Description:

As a result of guidelines from the CT plenary, CT1 has worked on a CR to introduce I-WLAN as a valid access technology for IMS.

CT1 has agreed on a CR that introduce I-WLAN over IMS in Release 6. This CR comprise the following:

1. Access to IMS is IPv6 only although the WLAN itself may be capable of IPv4;
2. WLAN tunnels are used to access IMS, and these are assumed to be used in the same manner as general purpose PDP contexts;
3. P-CSCF discovery is performed using DHCP only, and there is no I-WLAN specific mechanism provided;
4. There is no WLAN specific coding of the P-Access-Network-ID header beyond identification of the access technology;
5. There are no I-WLAN specific charging parameters carried to IMS;
6. Media grouping (separate streams) is not available;
7. Service based local policy and use of the media authorization token is not available;
8. There is no dedicated bearer for SIP signalling; and
9. The QoS requirements do not apply for I-WLAN.

CT1 would like to indicate that solutions for generic text for the bullets 6, 7, 8 and 9 are more restrictive than that specified in 23.228 as required for all access technologies but assumes that the solution outlined by CT1 is according to the intention of 23.228.

### 2. Actions:

**To SA2 group.**

**ACTION:**

CT1 hope the chosen solution will be in line with future extensions of IMS and not cause backwards compatibility issues.

CT1 ask SA2 investigate whether changes are required to 23.228 as a result of the above decisions.

### 3. Date of Next TSG-CN1 Meetings:

| | | |
|---|---|---|
| CT1_39 | 29th August – 2nd September 2005 | London, UK |

**3GPP TSG-CT1 Meeting #38** **Tdoc C1-050729**
**Cancun, Mexico, 25-29 April 2005**

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **24.229 CR 872** ⌘ **rev 2** ⌘ Current version: **6.6.0** ⌘

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | I-WLAN information for IMS | | |
| ***Source:*** | ⌘ | Nokia, Lucent | | |
| ***Work item code:*** | ⌘ | WLAN | ***Date:*** ⌘ | 27/04/2005 |
| ***Category:*** | ⌘ | **B** | ***Release:*** ⌘ | Rel-6 |

*Use one of the following categories:*
**F** *(correction)*
**A** *(corresponds to a correction in an earlier release)*
**B** *(addition of feature),*
**C** *(functional modification of feature)*
**D** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

***Reason for change:*** ⌘ According to the CT plenary exceptions, IMS over WLAN description is a requirement for Rel-6 and we have an extension to get it included.

The purpose of this CR is to accomplish this vis modifications to 3GPP TS 24.229

The technical assumptions behind this proposal are as follows:

- access to IMS is IPv6 only;
- only one WLAN tunnel is available for IMS access, and this tunnel is assumed to be used in the same manner as a general purpose PDP context;
- No specific QoS functionality is available
- P-CSCF discovery is performed using DHCP only;
- media grouping is not available;
- service based local policy and use of the media authorization token is not available;
- there is no WLAN specific coding of the P-Access-Network-ID header beyond identification of the access technology;
- there are no WLAN specific charging parameters carried to IMS.
- only 802.11a and 802.11b are supported in the coding, as these are the currently defined values in RFC 3455

***Summary of change:*** ⌘ A new annex X is created documenting I-WLAN access technology specific procedures. Descriptions of how P-Access-Network-Info and P-Charging-Info headers are treated for the varying access technologies are added back into the main body of the text in sections used in Rel-5 (sections 7.2A.4 & 7.2A.5) ), and

| | | |
|---|---|---|
| | | the text aligned where appropriate with the original release 5 text. The GPRS IP CAN case description for these headers that was in Annex B is included there and removed from Annex B.<br>Appropriate references are included in the main body of the text to this new document structure and |
| ***Consequences if not approved:*** | ⌘ | IMS usage over I-WLAN not described in Rel-6 specifications |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, 3.2, 3.2. 5.1.1.2, 5.1.1.3, 5.1.1.4, 5.1.1.6, 5.1.2A.1, 5.1.2A.2, 7.2A.4, 7.2A5, annex B.4.1, B.3.3.1, annex X added. | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

-------------------- FIRST CHANGE------------------

# 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] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[7A] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8C] 3GPP TS 24.234: "3GPP System to Wireless Local Area Network (WLAN) interworking; User Equipment (UE) to network protocols; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[11B] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks".

[11C] 3GPP TS 29.161: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services with Wireless Local Access and Packet Data Networks (PDN "

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[13A] 3GPP TS 29.209: "Policy control over Gq interface".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[19A] 3GPP TS 33.210: "IP Network Layer Security".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".

[20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".

[20C] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".

[20D] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[20E] RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 3966 (December 2004): "The tel URI for Telephone Numbers".

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".

[28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".

[29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".

[30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".

[33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".

[37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[39] draft-ietf-mmusic-sdp-new-13 (May 2003): "SDP: Session Description Protocol".

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

[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".

[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56B] RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)"

[57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[58] draft-ietf-sip-session-timer-15 (November 2004): "Session Timers in the Session Initiation Protocol (SIP)".

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

[59] RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[60] RFC 3891 (September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

[61] RFC 3911 (October 2004): "The Session Inititation Protocol (SIP) "Join" Header".

[62] RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

[63] RFC 3861 (August 2004): "Address Resolution for Instant Messaging and Presence".

[64] draft-ietf-sip-rfc3312-update-03 (September 2004): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

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

[70] RFC 3903 (October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[71] Void.

[72] RFC 3857 (August 2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".

[74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[75] draft-ietf-simple-event-list-04 (June 2003): "A Session Initiation Protocol (SIP) Event Notification Extension for Collections".

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

[77] draft-ietf-sipping-config-framework-05 (October 2004): "A Framework for Session Initiation Protocol User Agent Profile Delivery".

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

[78] draft-ietf-sipping-conference-package-03 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Conference State"

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

[79] draft-ietf-rohc-sigcomp-sip-01 (February 2004): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

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

[YY] 3GPP TS 23.234: "3GPP system to Wireles Local Area Network (WLAN) interworking; System description".

-------------------- NEXT CHANGE-----------------

## 3.1 Definitions

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

**Newly established set of security associations**: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF after the 200 (OK) response to a REGISTER request was received.

**Old set of security associations:** Two pairs of IPsec security associations still in existence after another set of security associations has been established due to a successful authentication procedure.

**Temporary set of security associations:** Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF, after an authentication challenge within a 401 (Unauthorized) response to a REGISTER request was received. The SIP level lifetime of such created security associations will be equal to the value of reg-await-auth timer.

**Integrity protected:** See 3GPP TS 33.203 [19]. Where a requirement exists to send information "integrity protected" the mechanisms specified in 3GPP TS 33.203 [19] are used for sending the information. Where a requirements exists to check that information was received "integrity protected", then the information received is checked for compliance with the procedures as specified in 3GPP TS 33.203 [19].

For the purposes of the present document, the following terms and definitions given in RFC 1594 [20B].

**Fully-Qualified Domain Name (FQDN)**

For the purposes of the present document, the following terms and definitions given in RFC 3261 [26] apply (unless otherwise specified see clause 6).

**Back-to-Back User Agent (B2BUA)**
**Client**
**Dialog**
**Final response**
**Header**
**Header field**
**Loose routeing**
**Method**
**Option-tag** (see RFC 3261 [26] subclause 19.2)
**Provisional response**
**Proxy, proxy server**
**Redirect server**
**Registrar**
**Request**
**Response**
**Server**
**Session**
**(SIP) transaction**
**Stateful proxy**
**Stateless proxy**
**Status-code** (see RFC 3261 [26] subclause 7.2)
**Tag** (see RFC 3261 [26] subclause 19.3)
**Target Refresh Request**
**User agent client (UAC)**
**User agent server (UAS)**
**User agent (UA)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4.1.1.1 and subclause 4a.7 apply:

**Breakout Gateway Control Function (BGCF)**
**Call Session Control Function (CSCF)**
**Home Subscriber Server (HSS)**
**Media Gateway Control Function (MGCF)**
**Multimedia Resource Function Controller (MRFC)**
**Multimedia Resource Function Processor (MRFP)**
**Subscription Locator Function (SLF)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclause 3.1 apply:

**Filter criteria**
**Initial filter criteria**
**Initial request**
**Standalone transaction**
**Subsequent request**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclauses 3.1, 4.3.3.1, 4.3.6, 4.6 and 5.4.12.1 apply:

**Interrogating-CSCF (I-CSCF)**
**IMS Application Level Gateway (IMS-ALG)**
**IP-Connectivity Access Network (IP-CAN)**
**Policy Decision Function (PDF)**
**Private user identity**
**Proxy-CSCF (P-CSCF)**
**Public Service Identity (PSI)**
**Public user identity**
**Serving-CSCF (S-CSCF)**
**Statically pre-configured PSI**

For the purposes of the present document, the following terms and definitions given in 3GPP TR 33.203 [19] apply:

**IM Subscriber Identity Module (ISIM)**
**Protected server port**
**Protected client port**

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [1] apply:

**Universal Integrated Circuit Card (UICC)**
**Universal Subscriber Identity Module (USIM)**
**User Equipment (UE)**

For the purposes of the present document, the following terms and definitions given in RFC 2401 [20A] Appendix A apply:

**Security association**

NOTE: A number of different security associations exist within the IM CN subsystem. Within this document the term specifically applies to the security association that exists between the UE and the P-CSCF, as this is the only security association that has direct impact on SIP.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [1B] apply:

**WLAN UE**
**3GPP AAA proxy**
**3GPP AAA server**
**Packet Data Gateway (PDG)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [7A] apply.

**Interworking WLAN**

For the purposes of the present document, the following terms and definitions given in ITU-T E.164 [57] apply:

**International public telecommunication number**

------------------- NEXT CHANGE-----------------

## 3.2 Abbreviations

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

| | |
|---|---|
| 1xx | A status-code in the range 101 through 199, and excluding 100 |
| 2xx | A status-code in the range 200 through 299 |
| AAA | Authentication, Authorization and Accounting |
| AS | Application Server |
| APN | Access Point Name |
| AUTN | Authentication TokeN |

| | |
|---|---|
| B2BUA | Back-to-Back User Agent |
| BGCF | Breakout Gateway Control Function |
| c | conditional |
| CCF | Charging Collection Function |
| CDR | Charging Data Record |
| CK | Ciphering Key |
| CN | Core Network |
| CSCF | Call Session Control Function |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| DTD | Document Type Definition |
| ECF | Event Charging Function |
| FQDN | Fully Qualified Domain Name |
| GCID | GPRS Charging Identifier |
| GGSN | Gateway GPRS Support Node |
| GPRS | General Packet Radio Service |
| HSS | Home Subscriber Server |
| i | irrelevant |
| I-CSCF | Interrogating CSCF |
| ICID | IM CN subsystem Charging Identifier |
| IK | Integrity Key |
| IM | IP Multimedia |
| IMS | IP Multimedia core network Subsystem |
| IMS-ALG | IMS Application Level Gateway |
| IMSI | International Mobile Subscriber Identity |
| IOI | Inter Operator Identifier |
| IP | Internet Protocol |
| IP-CAN | IP-Connectivity Access Network |
| IPsec | IP security |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| ISC | IP Multimedia Subsystem Service Control |
| ISIM | IM Subscriber Identity Module |
| I-WLAN | Interworking – WLAN |
| m | mandatory |
| MAC | Message Authentication Code |
| MCC | Mobile Country Code |
| MGCF | Media Gateway Control Function |
| MGW | Media Gateway |
| MNC | Mobile Network Code |
| MRFC | Multimedia Resource Function Controller |
| MRFP | Multimedia Resource Function Processor |
| PDG | Packet Data Gateway |
| PDP | Packet Data Protocol |
| PLMN | Public Land Mobile Network |
| PSTN | Public Switched Telephone Network |
| n/a | not applicable |
| NAI | Netework Access Identifier |
| o | optional |
| P-CSCF | Proxy CSCF |
| PDU | Protocol Data Unit |
| PSI | Public Service Identity |
| QoS | Quality of Service |
| RAND | RANDom challenge |
| RES | RESponse |
| RTCP | Real-time Transport Control Protocol |
| RTP | Real-time Transport Protocol |
| S-CSCF | Serving CSCF |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SLF | Subscription Locator Function |
| SQN | SeQuence Number |

| | |
|---|---|
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UE | User Equipment |
| UICC | Universal Integrated Circuit Card |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UDVM | Universal Decompressor Virtual Machine |
| USIM | Universal Subscriber Identity Module |
| WLAN | Wireless Local Area Network |
| x | prohibited |
| XMAC | expected MAC |
| XML | eXtensible Markup Language |

-------------------- NEXT CHANGE------------------

# 3A Interoperability with different IP-CAN

The IM CN subsystem can be accessed by UEs resident in different types of IP-CAN. The main body of this document, and annex A, are general to UEs and IM CN subsystems that are accessed using any type of IP-CAN. Requirements that are dependent on the type of IP-CAN are covered in annexes B and X~~,~~ or in separate specifications.

-------------------- NEXT CHANGE------------------

### 5.1.1.2 Initial registration

The UE can register a public user identity with its contact address at any time after it has aquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field, set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

i) the Supported header containing the option tag "path"; and

j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology ~~(for GPRS see subclause B.3).~~ (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;

e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

### 5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680 [43].

The UE shall use the default public user identiy for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header set to a SIP URI that contains the public user identity used for subscription;

c) a To header set to a SIP URI that contains the public user identity used for subscription;

d) an Event header set to the "reg" event package;

e) an Expires header set to 600 000 seconds as the value desired for the duration of the subscription

f) a P-Access-Network-Info header set as specified for the access network technology ~~(for GPRS see subclause B.3)~~(see subclause 7.2A.4); and

g) a Contact header set to contain the same IP address or FQDN, and with the protected server port value as in the initial registration.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header of the received response.

If continued subscription is required, the UE shall automatically refresh the subscription by the reg event package, for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less.

### 5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity with its contact address at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 [62].

The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

i) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

j) the Supported header containing the option tag "path"; and

k) the P-Access-Network-Info header set as specified for the access network technology ~~(for GPRS see subclause B).~~(see subclause 7.2A.4)

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the new expiration time of the registration for this public user identity found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

When the timer F expires at the UE, the UE shall:

1) stop processing of all ongoing dialogs and transactions and silently discard them locally; and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE may:

   a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

   b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

   c) perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 4: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

After a maximum of 5 consecutive initial registration attempts, the UE shall not automatically attempt any further initial registration for an implementation dependant time of at least 30 minutes.

-------------------- NEXT CHANGE------------------

### 5.1.1.6 User-initiated deregistration

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

The UE shall integrity protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if one is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field, set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be deregistered;

c) a To header set to the SIP URI that contains the public user identity to be deregistered;

d) a Contact header set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and the protected server port value bound to the security association;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

f) an Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

g) a Request-URI set to the SIP URI of the domain name of the home network; and

h) a P-Access-Network-Info header set as specified for the access network technology ~~(for GPRS see subclause B.3~~ (see subclause 7.2A.4~~see subclause X.1~~).

On receiving the 200 (OK) response to the REGISTER request, the UE shall remove all registration details relating to this public user identity.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and the security association is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered), the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

-------------------- NEXT CHANGE------------------

#### 5.1.2A.1 Mobile-originating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP response that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Preferred-Identity header:

- a public user identity which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration that was not subsequently deregistered or has expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header.

NOTE 2: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header.

NOTE 3: A number of headers can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header to "Anonymous".

NOTE 4: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header other than Anonymous.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

The UE shall insert a P-Access-Network-Info header into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology (~~for GPRS see subclause B.~~ see subclause 7.2A.4~~3~~).

NOTE 5: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected server port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 6: It is an implementation option whether these actions are also triggered by other means.

### 5.1.2A.2 Mobile-terminating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any response, the UE shall:

- include the protected server port in any Contact header that is otherwise included.

The UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 1: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Preferred-Identity in the form of a hint.

NOTE 2: A number of headers can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

The UE shall insert a P-Access-Network-Info header into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method. The UE shall populate the P-Access-Network-Info header with its current point of attachment to the IP-CAN as specified for the access network technology (~~for GPRS see subclause B.~~ see subclause 7.2A.4~~3~~).

-------------------- NEXT CHANGE------------------

## 7.2A.4 ~~Void~~ P-Access-Network-Info header

### 7.2A4.1 Introduction

The P-Access-Network-Info header is extended to include specific information relating to particular access technologies.

### 7.2A4.2 Syntax

The syntax of the P-Access-Network-Info header is described in RFC 3455 [52].

### 7.2A4.3 Additional coding rules for P-Access-Network-Info header

The UE shall populate the P-Access-Network-Info header, where use is specified in subclause 5.1, with the following contents:

1) the access-type field set to one of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-CDMA2000", "IEEE-802.11a" or "IEEE-802.11b" as appropriate to the radio access technology in use.

2) if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:

   Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);

3) if the access type field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits).

4) if the access-type field set to one of "IEEE-802.11a" or "IEEE-WLAN-802.11b" the access info parameter is set to a null value. This release of this specification does not define values for use in this parameter

-------------------- NEXT CHANGE------------------

## 7.2A.5 P-Charging-Vector header

### 7.2A.5.1 Introduction

The P-Charging-Vector header field is extended to include specific charging correlation information needed for IM CN subsystem functional entities.

### 7.2A.5.2 Syntax

#### 7.2A5.2.1 General

The syntax of the P-Charging-Vector header field is described in RFC 3455 [52]. There may be additional coding rules for this header depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.3 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

**Table 7.3: Syntax of extensions to P-Charging-Vector header**

```
   access-network-charging-info = (gprs-charging-info / i-wlan-charging-info / generic-param)
   gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)
   ggsn = "ggsn" EQUAL gen-value
   pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT
   pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]
   pdp-item = "pdp-item" EQUAL DIGIT
   pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
   gcid = "gcid" 1*HEXDIG
   auth-token = "auth-token" EQUAL 1*HEXDIG
   flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT
        "}")")"
   extension-param = token [EQUAL token]
   i-wlan-charging-info = "pdg"
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

The access-network-charging-info parameter includes alternative definitions for different types access networks. The description of these parameters are given in the subsequent subclauses.

The access network charging information is not included in the P-Charging-Vector for SIP signalling that is not associated with a session,

When the access network charging information is included in the P-Charging-Vector and necessary information is not available from the Go/Gq interface reference points then null or zero values are included

#### 7.2A5.2.2 GPRS as IP-CAN

GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter), media authorization token (auth token parameter), and a pdp-info parameter that contains the information for one or more PDP contexts. The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, and flow-id). The value of the pdp-item is a unique number that identifies each of the PDP-related charging information within the P-Charging-Vector header. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the PDP context charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.207 [12] Annex C. The gcid, ggsn address and flow-id parameters are transferred from the GGSN to the P-CSCF via the PDF over the Go interface (see 3GPP TS 29.207 [12]) and Gq interface (see 3GPP TS 29.209 [13A]).

The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.207 [12]). The P-CSCF shall encode it in hexadecimal format before include it into the gcid parameter. On receipt of this header, a node receiving a gcid shall decode from hexadecimal into binary format.

The access network charging information is not included in the P-Charging-Vector for SIP signalling may not be available for sessions that use a general purpose PDP context (for both SIP signalling and media) or that do not require media authorisation.

#### 7.2A5.2.3 I-WLAN as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

This version of the specification defines the use of "pdg" for inclusion in the P-Charging-Vector header. No other extensions are defined for use in I-WLAN in this version of the specification.

-------------------- NEXT CHANGE------------------

### 9.2.2 Handling of the IP-CAN

The UE shall ensure that appropriate resources are available for the media flow(s) on the IP-CAN(s) related to a SIP-session. The means to ensure this is dependant on the characteristics for each IP-CAN, and is described separately for each IP-CAN in question.

GPRS is described in annex B. I-WLAN is described in annex X.

-------------------- NEXT CHANGE------------------

#### B.3.1.1 ~~Additional coding rules for P-Access-Network-Info header~~Void

.~~The UE shall populate the P-Access-Network-Info header, where use is specified in subclause 5.1, with the following contents:~~

1) ~~the access-type field set to one of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000" as appropriate to the radio access technology in use;~~

2) ~~if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:~~

   ~~Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);~~

3) ~~if the access type field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:~~

   ~~Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits).~~

------------------- NEXT CHANGE-----------------

### B.4.1 ~~P-Charging-Vector header~~Void

~~The access network charging information is populated in the P-Charging-Vector using the gprs-charging-info parameter. Table B.1 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52]~~.

**~~Table B.1: Syntax of extensions to P-Charging-Vector header~~**

```
~~    access-network-charging-info = (gprs-charging-info / generic-param)~~
~~    gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)~~
~~    ggsn = "ggsn" EQUAL gen-value~~
~~    pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT~~
~~    pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]~~
~~    pdp-item = "pdp-item" EQUAL DIGIT~~
~~    pdp-sig = "pdp-sig" EQUAL ("yes" / "no")~~
~~    gcid = "gcid" 1*HEXDIG~~
~~    auth-token = "auth-token" EQUAL 1*HEXDIG~~
~~    flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT~~
~~          "}")")"~~
~~    extension-param = token [EQUAL token]~~
```

~~The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.~~

~~The access-network-charging-info parameter includes alternative definitions for different types access networks.~~

~~GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter), media authorization token (auth-token parameter), and a pdp-info parameter that contains the information for one or more PDP contexts. The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, and flow-id). The value of the pdp-item is a unique number that identifies each of the PDP-related charging information within the P-Charging-Vector header. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the PDP context charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.207 [12] Annex C. The gcid, ggsn address and flow-id parameters are transferred from the GGSN to the P-CSCF via the PDF over the Go interface (see 3GPP TS 29.207 [12]) and Gq interface (see 3GPP TS 29.209 [13A]).~~

~~The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.207 [12]). The P-CSCF shall encode it in hexadecimal format before include it into the gcid parameter. On receipt of this header, a node receiving a gcid shall decode from hexadecimal into binary format.~~

~~The access network charging information is not included in the P-Charging-Vector for SIP signalling that is not associated with a session, and may not be available for sessions that use a general purpose PDP context (for both SIP signalling and media) or that do not require media authorisation.~~

~~When the access network charging information is included in the P-Charging-Vector and necessary information is not available from the Go/Gq interface reference points then null or zero values are included.~~

------------------- NEXT CHANGE-----------------

# Annex X (normative): IP-Connectivity Access Network specific concepts when using I-WLAN to access IM CN subsystem

## X.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is Wireless LAN Interworking (I-WLAN).

## X.2 I-WLAN aspects when connected to the IM CN subsystem

### X.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by I-WLAN to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the PDG in support of this communication are specified in 3GPP TS 29.161 [11C]. When using the I-WLAN, the IP-CAN bearer is provided by an I-WLAN tunnel.

### X.2.2 Procedures at the UE

#### X.2.2.1 I-WLAN tunnel activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

a) Perform I-WLAN network selection i.e. gaining 3GPP Direct access as described in 3GPP TS 24.234 [8C] in the access dependent case;

b) Establish an I-WLAN tunnel with the PDG according to the W-APN and PDG selection criteria described in 3GPP TS 24.234 [8C]. The I-WLAN tunnel shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration.;

The I-WLAN tunnel shall carry both signalling and media i.e. it shall be a general-purpose. I-WLAN tunnel.

Note: Only one I-WLAN tunnel is available therefore no dedicated I-WLAN tunnel for signalling is possible.

c) Acquire a P-CSCF address(es).

The method for P-CSCF discovery is:

Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] as described in subclause 9.2.1.

If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 [40]

## X.2.2.2 I-WLAN tunnel procedures

### X.2.2.2.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same I-WLAN tunnel.

### X.2.2.2.2 Usage of I-WLAN tunnel for media

The UE may freely group media streams to the existing I-WLAN tunnel in case no indication of grouping of media streams is received from the P-CSCF.

If the UE receives media grouping attributes in accordance with RFC 3524[54] that it cannot provide within a single I-WLAN tunnel, then the UE shall handle such SDP offers in accordance with RFC 3388[53].

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, the UE shall reuse the existing I-WLAN tunnel and ignore the media authorization token.

### X.2.2.2.3 Special requirements applying to forked responses

Since the UE is unable to perform bearer modification, forked responses place no special requirements on the UE.

.------------------- NEXT CHANGE------------------

**3GPP TSG-CN1 Meeting #38 Tdoc C1-050741**
**Cancun, Mexico, 25-29 April 2005**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **23.009** | **CR** | **105** | ⌘**rev** | **1** | ⌘ | Current version: | **6.0.0** | ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Directed Retry Handover for Bearer Service | | |
| ***Source:*** | ⌘ | Vodafone, Nokia | | |
| ***Work item code:*** | ⌘ | CS_VSS | ***Date:*** ⌘ | 27/04/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | 22.129 clause 5.2 states, "In order to allow the connection with the negotiated bearer- or teleservice to be established, means shall be defined, which makes it possible for the core network, to recommend to access network to handover the UE to another RAT better suited to support the desired bearer- or teleservice."<br>Two cases exist that require this behaviour:<br>- A UE attached to GSM and engaged in a voice call might request to switch to a video call, as described in step number 8) of clause 4.2.1 of TR 23.903 v6.1.0. If GSM is unable to provide a 64 kbit/s bearer, an inter-system handover to UMTS is required.<br>- A dual mode UE supporting transparent bearer services, e.g. CS multimedia, in UMTS but not in GSM, attached in a GSM radio network can request a multimedia call. Consequently, the network must perform an intersystem handover to make the call setup successful.<br>Information elements have been added in TS 48.008 clause 3.2.2.75 (Tdoc P-00-195, CR A205) and TS 25.413 clause 9.2.1.41 (Tdoc RP-000695 CR 206) to provide intersystem handover.<br>23.009 does not currently include the case where handover is necessary due to the inability of GSM to support the requested bearer, or handover to GSM due to network preference. |
| ***Summary of change:*** | ⌘ | The option for the network to request handover from GSM to UMTS because a bearer was requested that is not supported in GSM is added.<br>The option for the network to request handover from UMTS to GSM because of network preference is added. |

| | | |
|---|---|---|
| ***Consequences if not approved:*** | ⌘ | UEs capable of switching from a voice to a video call will be unable to do so if attached to GSM.<br>Most/many dual mode UEs supporting CS multimedia are not expected to support it in GSM (where ECSD is required for 64 kbit/s). Without a correction in the specifications a multimedia call is not possible if the UE happens to be attached to GSM.<br>A network will be unable to handover from UMTS to GSM even though this would be better suited to providing the requested bearer service. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 14.2, 14.3 | | | | |
| | | Y | N | | | |
| ***Other specs affected:*** | ⌘ | X | | Other core specifications | ⌘ | 24.008 CR937 |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

# 14 Directed retry handover

Editor's Note: [Directed retry in the cases of SRNS relocation is FFS]

## 14.1 GSM handover

The directed retry procedure allows the network to select the optimum cell for the Mobile Station. The process of directed retry involves the assignment of a Mobile Station to a radio channel on a cell other than the serving cell. This process is triggered by the assignment procedures, as described in 3GPP TS 08.08 [5], and employs internal or external handover procedures as described in clauses 6 and 7. The successful procedure for a directed retry is as shown in figure 40 and as described below.

If during the assignment phase, as represented by the A-ASSIGNMENT-REQUEST message, a handover becomes necessary, due to either radio conditions or congestion, then the Mobile Station may be handed over to a different cell. When the decision has been made to handover the MS the BSS-A may send an A-ASSIGNMENT-FAILURE message, indicating 'directed retry', before sending the A-HANDOVER-REQUIRED message to MSC-A, indicating 'directed retry'. However BSS-A may alternatively send the A-HANDOVER-REQUIRED message, indicating 'directed retry', without sending the A-ASSIGNMENT-FAILURE message. Other cause values may be used instead of "Directed Retry" in the A-HANDOVER-REQUIRED message, this will allow the MSC to take different actions dependent on the received cause. Upon receipt of the A-HANDOVER-REQUIRED message from BSS-A, then MSC-A shall initiate the handover as described in clauses 6 and 7. No resources shall be cleared in the MSC-A or BSS-A for this connection.

After receipt of the A-HANDOVER-COMPLETE message from BSS-B the assignment procedure shall be considered to be complete and the resources on BSS-A shall be cleared.

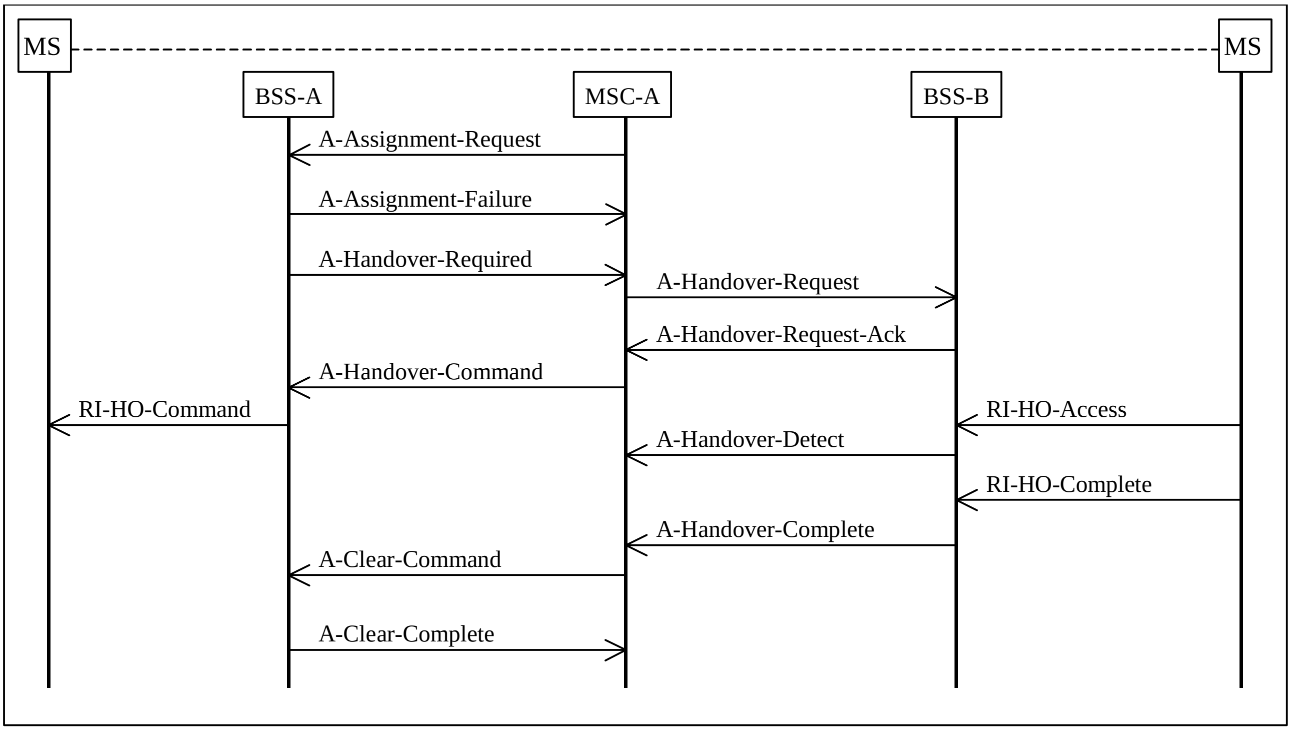


**Figure 40: Example of a Directed Retry Intra-MSC Handover Procedure**

If a failure occurs during the handover attempt, for example A-HANDOVER-FAILURE returned from BSS-A or BSS-B, then MSC-A will terminate the handover to BSS-B. Under these conditions MSC-A may optionally take one of a number of actions:

i) retry the handover to the same cell;

ii) select the next cell from the list contained in the A-HANDOVER-REQUIRED message and attempt a handover to the new cell;

iii) send an A-HANDOVER-REQUIRED-REJECT to BSS-A, if an A-HANDOVER-COMMAND has not already been sent;

iv) retry the assignment procedure to BSS-A, if the failure message was returned from BSS-A. This option is additional to those for normal handover;

v) Clear the complete call.

The procedures for Inter-MSC handover are also applicable to the directed retry process. If an Inter-MSC handover is necessary then the assignment process should be considered to have completed successfully upon receipt of the A-HO-COMPLETE included in the MAP-SEND-END-SIGNAL request.

## 14.2 GSM to UMTS handover

The directed retry procedure allows the network to select the optimum cell for the UE/MS. The process of directed retry involves the assignment of a UE/MS to a radio channel on a cell other than the serving cell. This process is triggered by the assignment procedures, as described in 3GPP TS 08.08 [5], and employs internal or external GSM to UMTS handover procedures as described in clauses 6.2.2 and 8.2. The successful procedure for a directed retry in case of an intra-3G_MSC GSM to UMTS handover is as shown in figure 40a and as described below.

If during the assignment phase, as represented by the A-ASSIGNMENT-REQUEST message, a GSM to UMTS handover becomes necessary, due to ~~either~~ radio conditions ~~or~~, congestion or inability to provide the requested bearer service in GSM, then the UE/MS may be handed over to a UMTS cell. If the requested bearer service cannot be provided in GSM, 3G_MSC-A shall indicate in the A-ASSIGNMENT-REQUEST message that handover to UMTS should be performed. When the decision has been made to handover the UE/MS the BSS-A may send an A-ASSIGNMENT-FAILURE message, indicating 'directed retry', before sending the A-HANDOVER-REQUIRED message to 3G_MSC-A, indicating 'directed retry'. However BSS-A may alternatively send the A-HANDOVER-REQUIRED message, indicating 'directed retry', without sending the A-ASSIGNMENT-FAILURE message. Other cause values may be used instead of "Directed Retry" in the A-HANDOVER-REQUIRED message, this will allow the 3G_MSC to take different actions dependent on the received cause. Upon receipt of the A-HANDOVER-REQUIRED message from BSS-A, then 3G_MSC-A shall initiate the GSM to UMTS handover as described in clauses 6.2.2 and 8.2. No resources shall be cleared in the 3G_MSC-A or BSS-A for this connection.

After receipt of the Iu-RELOCATION-COMPLETE message from RNS-B the assignment procedure shall be considered to be complete and the resources on BSS-A shall be cleared.

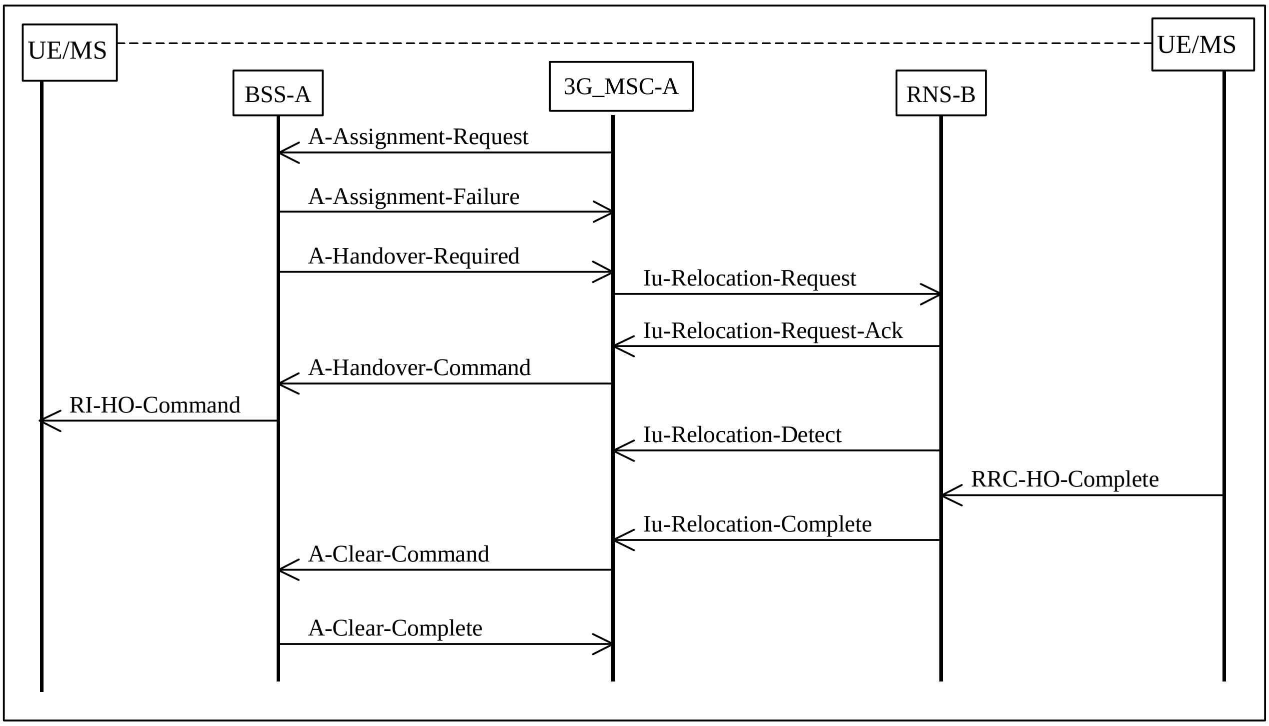


**Figure 40a: Example of a Directed Retry Intra-3G_MSC GSM to UMTS Handover Procedure**

If a failure occurs during the handover attempt, for example A-HANDOVER-FAILURE returned from BSS-A or Iu-RELOCATION FAILURE from RNS-B then 3G_MSC-A will terminate the GSM to UMTS handover to RNS-B. Under these conditions 3G_MSC-A may optionally take one of a number of actions:

i) send an A-HANDOVER-REQUIRED-REJECT to BSS-A, if an A-HANDOVER-COMMAND has not already been sent;

ii) retry the assignment procedure to BSS-A, if the failure message was returned from BSS-A. This option is additional to those for normal handover;

iii) Clear the complete call.

The procedures for Inter-3G_MSC GSM to UMTS handover are also applicable to the directed retry process. If an Inter-3G_MSC GSM to UMTS handover is necessary then the assignment process should be considered to have completed successfully upon receipt of the A-HO-COMPLETE included in the MAP-SEND-END-SIGNAL request.

## 14.3 UMTS to GSM handover

The directed retry procedure allows the network to select the optimum cell for the UE/MS. The process of directed retry involves the assignment of a UE/MS to a radio channel on a cell other than the serving cell. This process is triggered by the assignment procedures, as described in 3GPP TS 25.413 [1], and employs UMTS to GSM handover procedures as described in clauses 6.2.1 and 8.1. The successful procedure for a directed retry in case of an intra-3G_MSC UMTS to GSM handover is as shown in figure 40b and as described below.

If during the assignment phase, as represented by the Iu-RAB-ASSIGNMENT-REQUEST message, a UMTS to GSM handover becomes necessary, due to either radio conditions ~~or~~, congestion or network preference, then the UE/MS may be handed over to a GSM cell. If the handover to GSM is required due to network preference, 3G_MSC-A shall indicate in the Iu-RAB-ASSIGNMENT-REQUEST message that handover to GSM should be performed. When the decision has been made to handover the UE/MS the RNS-A shall send an Iu-RAB-ASSIGNMENT-RESPONSE message, indicating 'directed retry', before sending the Iu-RELOCATION-REQUIRED message to 3G_MSC-A, indicating 'directed retry'. Other cause values may be used instead of "Directed Retry" in the Iu-RELOCATION-REQUIRED message, this will allow the 3G_MSC to take different actions dependent on the received cause. Upon receipt of the Iu-RELOCATION-REQUIRED message from RNS-A, then 3G_MSC-A shall initiate the UMTS to GSM handover as described in clauses 6.2.1 and 8.1. No resources shall be cleared in the 3G_MSC-A or RNS-A for this connection.

After receipt of the A-HANDOVER-COMPLETE message from BSS-B the assignment procedure shall be considered to be complete and the resources on RNS-A shall be cleared.

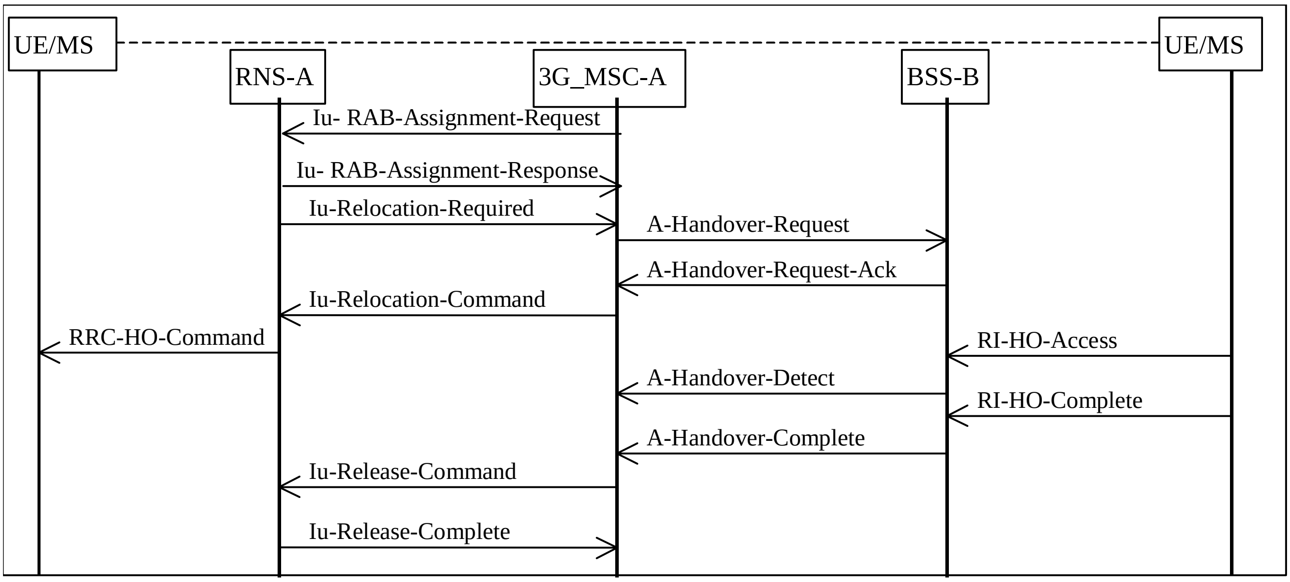


**Figure 40b: Example of a Directed Retry Intra-3G_MSC UMTS to GSM Handover Procedure**

If a failure occurs during the handover attempt, for example Iu-RELOCATION FAILURE returned from RNS-A or A-HANDOVER-FAILURE from BSS-B then 3G_MSC-A will terminate the UMTS to GSM handover to BSS-B. Under these conditions 3G_MSC-A may optionally take one of a number of actions:

i) send an Iu-RELOCATION-PREPARATION FAILURE to RNS-A, if an Iu-RELOCATION-COMMAND has not already been sent;

ii) retry the assignment procedure to RNS-A, if the failure message was returned from RNS-A. This option is additional to those for normal handover;

iii) Clear the complete call.

The procedures for Inter-3G_MSC UMTS to GSM handover are also applicable to the directed retry process. If an Inter-3G_MSC UMTS to GSM handover is necessary then the assignment process should be considered to have completed successfully upon receipt of the A-HO-COMPLETE included in the MAP-SEND-END-SIGNAL request.

**3GPP TSG-CT1 Meeting #38** **Tdoc C1-050795**
**Cancun, Mexico, 25 – 29 April, 2005** **Revision of C1-050448, C1-050733**

*CR-Form-v7.1*

## CHANGE REQUEST

⌘ **24.008 CR 962** ⌘**rev** **2** ⌘ Current version: **6.8.0** ⌘

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Transparent data call request in dual mode case |
| ***Source:*** | ⌘ | Nokia |
| ***Work item code:*** | ⌘ | TEI-6 |
| ***Date:*** | ⌘ | 14/04/2005 |
| ***Category:*** | ⌘ | F |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | Service based handover has been defined in stage 1 and stage 2, but A dual mode UE supporting transparent bearer services, e.g. CS multimedia, in UMTS but not in GSM, attached in a GSM radio network, has no means to indicate to the network that it would like to set up such a call. Consequently, the network does not get the indication that service based intersystem handover should be initiated to make the call setup successful. |
| ***Summary of change:*** | ⌘ | By setting all Acceptable Channel Codings to 'Not Acceptable' in the call setup BCIE, the UE indicates to the network that the UE does not support the requested service in A/Gb or GERAN Iu mode, and an intersystem handover is needed before the call creation can proceed. Similarily, while in UTRAN Iu mode, the network gets informed that the UE does not support the service in A/G or GERAN Iu mode. |
| ***Consequences if not approved:*** | ⌘ | As part of the stage 3 for service based handover is missing, there use of the already defined other feature (video call) is restricted unnecessarily. Many dual mode UEs supporting CS multimedia are not expected to support it in GSM where symmetric ECSD 64 kbit/s support would be required. Without a correction in the specifications a multimedia call is not possible, if the UE happens to be attached to a GSM radio network. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, 5.3.6.2.1, 5.3.6.2.2, 10.5.4.5 | | | | |
| | | Y | N | | | |
| ***Other specs*** | ⌘ | X | | Other core specifications | ⌘ | 27.001, 48.008 |

| | | | | |
|---|---|---|---|---|
| ***affected:*** | | X | Test specifications | |
| | | X | O&M Specifications | |
| ***Other comments:*** | ⌘ | It is proposed to consider this CR as release independent and implementable on earlier releases too. | | |

**How to create CRs using this form:**

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks"  feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text.  Delete those parts of the specification which are not relevant to the change request.

# 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] Void.

[2] Void.

[2a] 3GPP TR 21.905 "Vocabulary for 3GPP Specifications"

[3] 3GPP TS 22.002: "Circuit Bearer Services (BS) supported by a Public Land Mobile Network (PLMN)".

[4] 3GPP TS 22.003: "Teleservices supported by a Public Land Mobile Network (PLMN)".

[5] 3GPP TS 42.009: "Security aspects".

[5a] 3GPP TS 33.102: "3G security; Security architecture".

[6] 3GPP TS 22.011: "Service accessibility".

[7] 3GPP TS 42.017: "Subscriber Identity Modules (SIM); Functional characteristics".

[8] 3GPP TS 22.101: "Service aspects; Service principles".

[8a] 3GPP TS 22.001: "Principles of circuit telecommunication services supported by a Public Land Mobile Network (PLMN)".

[8b] 3GPP TS 23.038: "Alphabets and language-specific information".

[9] 3GPP TS 23.101: "General UMTS Architecture".

[9a] 3GPP TS 23.108: "Mobile radio interface layer 3 specification core network protocols; Stage 2 (structured procedures)".

[10] 3GPP TS 23.003: "Numbering, addressing and identification".

[11] 3GPP TS 43.013: "Discontinuous Reception (DRX) in the GSM system".

[12] 3GPP TS 23.014: "Support of Dual Tone Multi-Frequency (DTMF) signalling".

[12a] ETSI ES 201 235-2, v1.2.1: "Specification of Dual Tone Multi-Frequency (DTMF); Transmitters and Receivers; Part 2: Transmitters".

[13] 3GPP TS 43.020: "Security-related network functions".

[14] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[15] 3GPP TS 24.002: "GSM-UMTS Public Land Mobile Network (PLMN) access reference configuration".

[16] 3GPP TS 44.003: "Mobile Station - Base Station System (MS - BSS) interface; Channel structures and access capabilities".

[17] 3GPP TS 44.004: "Layer 1; General requirements".

[18] 3GPP TS 44.005: "Data Link (DL) layer; General aspects".

[19] 3GPP TS 44.006: "Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification".

[19a] 3GPP TS 25.321: "Medium Access Control (MAC) protocol specification".

[19b] 3GPP TS 25.322: "Radio Link Control (RLC)  protocol specification".

[19c] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

[20] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[21] 3GPP TS 24.010: "Mobile radio interface layer 3; Supplementary services specification; General aspects".

[22] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[23] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[23a] 3GPP TS 44.071: "Location Services (LCS); Mobile radio interface layer 3 specification."

[23b] 3GPP TS 44.031 "Location Services LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC); Radio Resource LCS Protocol (RRLP)".

[23c] 3GPP TS 25.331: "Radio Resource Control (RRC) protocol specification"

[24] 3GPP TS 24.080: "Mobile radio Layer 3 supplementary service specification; Formats and coding".

[25] 3GPP TS 24.081: "Line identification supplementary services; Stage 3".

[26] 3GPP TS 24.082: "Call Forwarding (CF) supplementary services; Stage 3".

[27] 3GPP TS 24.083: "Call Waiting (CW) and Call Hold (HOLD) supplementary services; Stage 3".

[28] 3GPP TS 24.084: "MultiParty (MPTY) supplementary services; Stage 3".

[29] 3GPP TS 24.085: "Closed User Group (CUG) supplementary services; Stage 3".

[30] 3GPP TS 24.086: "Advice of Charge (AoC) supplementary services; Stage 3".

[31] 3GPP TS 24.088: "Call Barring (CB) supplementary services; Stage 3".

[32] 3GPP TS 45.002: "Multiplexing and multiple access on the radio path".

[33] 3GPP TS 45.005: "Radio transmission and reception".

[34] 3GPP TS 45.008: "Radio subsystem link control".

[35] 3GPP TS 45.010: "Radio subsystem synchronization".

[36] 3GPP TS 27.001: "General on Terminal Adaptation Functions (TAF) for Mobile Stations (MS)".

[36a] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services ".

[37] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[38] 3GPP TS 29.007: "General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)".

[39] 3GPP TS 51.010: "Mobile Station (MS) conformance specification".

[40] 3GPP TS 51.021: "GSM radio aspects base station system equipment specification".

[41] ISO/IEC 646 (1991): "Information technology - ISO 7-bit coded character set for information interchange".

[42] ISO/IEC 6429: "Information technology - Control functions for coded character sets".

[43] ISO 8348 (1987): "Information technology -- Open Systems Interconnection -- Network Service Definition".

[44] ITU-T Recommendation E.163: "Numbering plan for the international telephone service".

[45] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[46] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

[47] ITU-T Recommendation F.69 (1993): "The international telex service - Service and operational provisions of telex destination codes and telex network identification codes".

[48] ITU-T Recommendation I.330: "ISDN numbering and addressing principles".

[49] ITU-T Recommendation I.440 (1989): "ISDN user-network interface data link layer - General aspects".

[50] ITU-T Recommendation I.450 (1989): "ISDN user-network interface layer 3 General aspects".

[51] ITU-T Recommendation I.500 (1993): "General structure of the ISDN interworking recommendations".

[52] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".

[53] ITU Recommendation Q.931: ISDN user-network interface layer 3 specification for basic control".

[54] ITU-T Recommendation V.21: "300 bits per second duplex modem standardized for use in the general switched telephone network".

[55] ITU-T Recommendation V.22: "1200 bits per second duplex modem standardized for use in the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".

[56] ITU-T Recommendation V.22bis: "2400 bits per second duplex modem using the frequency division technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".

[57] Void.

[58] ITU-T Recommendation V.26ter: "2400 bits per second duplex modem using the echo cancellation technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".

[59] ITU-T Recommendation V.32: "A family of 2-wire, duplex modems operating at data signalling rates of up to 9600 bit/s for use on the general switched telephone network and on leased telephone-type circuits".

[60] ITU-T Recommendation V.110: "Support by an ISDN of data terminal equipments with V-Series type interfaces".

[61] ITU-T Recommendation V.120: "Support by an ISDN of data terminal equipment with V-Series type interfaces with provision for statistical multiplexing".

[62] ITU-T Recommendation X.21: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for synchronous operation on public data networks".

[63] Void.

[64] Void.

[65] ITU-T Recommendation X.30: "Support of X.21, X.21 bis and X.20 bis based Data Terminal Equipments (DTEs) by an Integrated Services Digital Network (ISDN)".

[66] ITU-T Recommendation X.31: "Support of packet mode terminal equipment by an ISDN".

[67] Void.

[68] Void.

[69] ITU-T Recommendation X.121: "International numbering plan for public data networks".

[70] ETSI ETS 300 102-1: "Integrated Services Digital Network (ISDN); User-network interface layer 3; Specifications for basic call control".

[71] ETSI ETS 300 102-2: "Integrated Services Digital Network (ISDN); User-network interface layer 3; Specifications for basic call control; Specification Description Language (SDL) diagrams".

[72] ISO/IEC 10646: "Information technology -- Universal Multiple-Octet Coded Character Set (UCS)".

[73] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service Description; Stage 1".

[74] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[75] 3GPP TS 43.064: "General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2".

[76] 3GPP TS 44.060: "General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/Medium Access Control (RLC/MAC) protocol".

[77] IETF RFC 1034: "Domain names - concepts and facilities".

[78] 3GPP TS 44.065: "Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[78a] 3GPP TS 44.064: "Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) Layer Specification".

[79] ITU Recommendation I.460: "Multiplexing, rate adaption and support of existing interfaces".

[80] 3GPP TS 26.111: "Codec for Circuit Switched Multimedia Telephony Service; Modifications to H.324".

[81] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[82] 3GPP TS 43.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[83] 3GPP TS 26.103: "Speech Codec List for GSM and UMTS".

[84] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[85] 3GPP TS 48.008: "Mobile-services Switching Centre – Base Station System (MSC – BSS) interface; layer 3 specification".

[86] 3GPP TS 48.018: "General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP)".

[87] 3GPP TS 43.055: "Dual Transfer Mode (DTM); Stage 2".

[88] 3GPP TS 23.067: "enhanced Multi-Level Precedence and Pre-emption service (eMLPP); Stage 2".

[88a] 3GPP TS 23.093: "Technical realization of Completion of Calls to Busy Subscriber (CCBS); Stage 2".

[89] 3GPP TS 22.042: "Network Identity and Time Zone (NITZ), Stage 1".

[90] 3GPP TS 23.040: "Technical realization of Short Message Service (SMS)".

[91] 3GPP TS 44.056: "GSM Cordless Telephony System (CTS), (Phase 1) CTS Radio Interface Layer 3 Specification".

[92] 3GPP TS 23.226: "Global Text Telephony; Stage 2 "

[93] 3GPP TS 26.226: "Cellular Text Telephone Modem (CTM), General Description "

[94] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes"

[95] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP"

[96] 3GPP TS 23.205: "Bearer-independent circuit-switched core network; Stage 2".

[97] 3GPP TS 23.172: "UDI/RDI Fallback and Service Modification; Stage 2".

[98] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode"

[99] RFC 3513 (April 2003): "Internet Protocol Version 6 (IPv6) Addressing Architecture".

[100] 3GPP TS 29.207: "Policy control over Go interface".

[101] 3GPP TS 21.111: "USIM and IC card requirements".

[102] RFC 1661 (July 1994): "The Point-to-Point Protocol (PPP)".

[103] RFC 3232 (January 2002): "Assigned Numbers: RFC 1700 is Replaced by an On-line Database".

[104] 3GPP TS 23.034: "High Speed Circuit Switched Data (HSCSD) – Stage 2".

[105] 3GPP TS 23.271: "Functional stage 2 description of LCS".

[106] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[107] RFC 3376 (October 2002): "Internet Group Management Protocol, Version 3".

[108] RFC 2710 (October 1999): "Multicast Listener Discovery (MLD) for IPv6".

[109] 3GPP TS 23.251: "Network Sharing; Architecture and Functional Description".

[110] 3GPP TS 25.346: “Introduction of the Multimedia Broadcast Multicast Service (MBMS) in the Radio Access Network”

[111] 3GPP TS 44.118: "Radio Resource Control (RRC) protocol; Iu mode".

[112] 3GPP TS 31.102: "Characteristics of the USIM Application".

[113] 3GPP TS 43.129: "Packet-switched handover for GERAN A/Gb mode; Stage 2".

[114] 3GPP TS 23.009: "Handover procedures".

### 5.3.6 Support of multimedia calls

#### 5.3.6.1 Service description

The 3GPP circuit-switched multimedia call is based on the 3G-324M [26.111], which is a 3GPP-variant of the ITU-T H.324 recommendation. CS Multimedia telephony is a Bearer Service, which utilizes the Synchronous Transparent Data service (BS30) [3].

At the multimedia call setup the required call type, 3G-324M, is indicated, for the network to be able to invoke appropriate interworking functionality. In the peer end the H.324 information is used to invoke the terminal application. In addition to H.324 indication the terminal must select Information Transfer Capability (ITC) for the multimedia call. The 'correct' ITC depends on the peer end and the transporting networks; an all-ISDN call is a UDI/RDI call, and a call, which involves PSTN, is an analog "3.1 kHz audio" call.

For the case when the setup of a multimedia call is not successful, fallback to speech is specified.

Users may also request a service change between UDI/RDI multimedia and speech modes during a call (see 3GPP TS 23.172 [97]).

#### 5.3.6.2 Call establishment

For both mobile originating and mobile terminating calls, the normal call establishment procedures apply, with the exceptions specified in the following subclauses.

For further description of the function of MSC/IWF in the following clauses, see 3GPP TS 29.007 [38].

##### 5.3.6.2.1 Mobile originated multimedia call establishment

At call setup the required call type, 3G-324M, is indicated by the originating MS in the SETUP message, with the *bearer capability IE* parameter Other Rate Adaptation set to "H.223 and H.245".

For analogue multimedia, the support of a fallback to speech is requested by including two *bearer capability IEs,* multimedia first and speech as the second BC in the SETUP message. The MS shall indicate fallback to speech by these two BC IEs and the associated Repeat Indicator set to "support of fallback".

For UDI/RDI multimedia, the support of a fallback and service change is requested by including two *bearer capability IEs*, with the first BC as the preferred service in the SETUP message. The MS shall indicate service change and fallback by these two BC IEs and the associated Repeat Indicator set to "support of service change and fallback".

If the *bearer capability IE* received from the MS indicates no A/Gb mode support for the requested bearer service, the network shall consider it as a request to perform an inter-system handover to UTRAN Iu mode, as described in TS 23.009 [114] subclause 14.2.

The bearer compatibility checking in the network is according to 5.3.4.2.1.

If the MS requested for an analogue multimedia call with fallback to speech, or for a UDI/RDI multimedia call with fallback and service change, and the network accepts the call, the network has the following options for the inclusion of *bearer capability IEs* in the CALL PROCEEDING message:

- if the network accepts the requested analogue multimedia call and supports fallback to speech, both multimedia and speech *bearer capability IEs* shall be included;
- if the network accepts the requested UDI/RDI multimedia call and supports fallback and service change, both multimedia and speech *bearer capability IEs* shall be included. The order of the *bearer capability* IEs determines the preferred service, and the network may reverse the order of these IEs (see 3GPP TS 23.172 [97], subclause 4.2.1);
- if the network accepts a multimedia (only) call, a multimedia *bearer capability IE* shall be included;
- if the network accepts a speech (only) call, a speech *bearer capability IE* shall be included;
- for a UDI/RDI multimedia call, if the network accepts the requested speech call and supports service change, both multimedia and speech *bearer capability IEs* shall be included. The order of the *bearer capability* IEs

determines the preferred service, and the network may reverse the order of these IEs (see 3GPP TS 23.172 [97], subclause 4.2.1);

- if the network received a UDI/RDI multimedia *bearer capability* IE with FNUR equal to 32kbit/s and a speech *bearer capability* IE in the SETUP message, the network shall not release the call, but shall reply with one *bearer capability* IE only, as specified in 3GPP TS 23.172 [97].

NOTE: Service change and fallback for UDI/RDI multimedia calls is not supported with Fixed Network User Rate set to 32 kbit/s (see 3GPP TS 23.172 [97]).

If the MS requested for a multimedia call only, and the network accepts the call, the network shall always include a single multimedia *bearer capability IE* in the CALL PROCEEDING message.

The originating user shall determine (possibly by pre-configuration of the terminal) whether a digital connection is required or if the call will be an analog modem call. If the call is expected to be digital the multimedia *bearer capability* IE parameter ITC is set to UDI/RDI. In an analog call the multimedia *bearer capability* IE parameter ITC is set to "3,1 kHz audio ex PLMN". Additionally required modem type is indicated (Other Modem Type = V.34).

#### 5.3.6.2.1.1 Fallback

If the network, during the setup of an H.324-call, detects that the transit network or the called end does not support an H.324 call (*e.g.* because of a failure in the modem handshaking in case of an analogue multimedia call), then the network initiates the in-call modification procedure (see subclause 5.3.4.3) towards the MS to modify the call mode to speech, if the MS had included a speech *bearer capability IE* in the SETUP message.

In case of a UDI/RDI multimedia call with service change and fallback, if the network detects that the called end does not support speech, then it initiates an in-call modification procedure towards the MS to modify the call mode to multimedia, if the first *bearer capability IE* was for a speech call.

### 5.3.6.2.2 Mobile terminating multimedia call

At call setup the required call type, 3G-324M, is indicated by the network in the SETUP message, with the *bearer capability IE* parameter. Other Rate Adaptation set to 'H.223 and H.245'. ITC is either '3,1 kHz audio ex PLMN' or 'UDI/RDI'.

For analogue multimedia, if the network supports fallback to speech and the subscriber has subscription to speech, two *bearer capability* IEs, multimedia first and speech as the second BC are included in the SETUP message. The network shall indicate fallback to speech by these two BC IEs and the associated Repeat Indicator set to "support of fallback".

For UDI/RDI multimedia, if the network supports fallback and service change, and the subscriber has subscription to speech, two *bearer capability IEs*, with the first BC as the preferred service are included in the SETUP message. The network shall indicate service change and fallback by these two BC IEs and the associated Repeat Indicator set to "service change and fallback".

If the *bearer capability IE* received from the MS indicates no A/Gb mode support for the requested bearer service, the network shall consider it as a request to perform an inter-system handover to UTRAN Iu mode, as described in TS 23.009 [114] subclause 14.2.

*The bearer capability IE(s)* may (in the case of the single numbering scheme) be missing from the SETUP message.

The bearer compatibility checking in the MS is according to 5.3.4.2.2.

The MS shall indicate the supported call type(s) in the CALL CONFIRMED message, which is the acknowledgement to SETUP. If the network offered an analogue multimedia call with fallback to speech, or a UDI/RDI multimedia call with fallback and service change, the MS has the following options for the inclusion of *bearer capability IEs* in the CALL CONFIRMED message:

- if the MS/user accepts the offered analogue multimedia call and supports fallback to speech, both multimedia and speech *bearer capability IEs* shall be included;
- if the MS/user accepts the offered UDI/RDI multimedia call, and supports fallback and service change, both multimedia and speech *bearer capability IEs* shall be included. The order of the BC IEs determines the preferred service, and the MS/user may reverse the order of these IEs;

- if the MS/user accepts the offered multimedia call, but does not support fallback or service change, only a multimedia *bearer capability IE* shall be included;

- if the MS/user wishes a speech (only) call a speech *bearer capability IE* is included;

- for a UDI/RDI multimedia call, if the MS/user accepts the offered speech call and supports service change, both speech and multimedia *bearer capability IEs* shall be included. The order of the BC IEs determines the preferred service, and the MS/user may reverse the order of these IEs.

If the network offered a multimedia call only, and the MS/user accepts the call, the MS shall always include a single multimedia *bearer capability IE* in the CALL CONFIRMED message.

If the SETUP contained no *bearer capability IE* the network shall perform compatibility checking of the CALL CONFIRMED message in the same way as the compatibility checking of the SETUP message in the mobile originating call case, described in subclause 5.3.6.2.1.

## 10.5.4.5 Bearer capability

The purpose of the bearer capability information element is to describe a bearer service. The use of the bearer capability information element in relation to compatibility checking is described in annex B.

The bearer capability information element is coded as shown in figure 10.5.88/3GPP TS 24.008 and tables 10.5.102/3GPP TS 24.008 to 10.5.115/3GPP TS 24.008.

The bearer capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 16 octets.

| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |
|---|---|---|---|---|---|---|---|---|
| | Bearer capability IEI | | | | | | | octet 1 |
| Length of the bearer capability contents | | | | | | | | octet 2 |
| 0/1<br>ext | radio<br>channel<br>requirement | | co-<br>ding<br>std | trans<br>fer<br>mode | information<br>transfer<br>capability | | | octet 3 |
| 0/1<br>ext | 0<br>co-<br>ding | CTM | 0<br>spare | speech version<br>indication | | | | octet 3a * |
| 0/1<br>ext | 0<br>co-<br>ding | 0<br>spare | 0<br>spare | Speech version<br>Indication | | | | octet 3b etc* |
| 1<br>ext | comp<br>-ress. | structure | | dupl.<br>mode | confi<br>gur. | NIRR | esta-<br>bli. | octet 4* |
| 0/1<br>ext | 0 0<br>access id. | | rate<br>adaption | | signalling<br>access protocol | | | octet 5* |
| 0/1<br>ext | Other ITC | | Other rate<br>adaption | | 0 0 0<br>Spare | | | octet 5a* |
| 1<br>ext | Hdr/<br>noHdr | Multi<br>frame | Mode | LLI | Assig<br>nor/e | Inb.<br>neg | 0<br>Spare | octet 5b* |
| 0/1<br>ext | 0 1<br>layer 1 id. | | User information<br>layer 1 protocol | | | | sync/<br>async | octet 6* |
| 0/1<br>ext | numb.<br>stop<br>bits | nego-<br>tia-<br>tion | numb.<br>data<br>bits | user rate | | | | octet 6a* |
| 0/1<br>ext | intermed.<br>rate | | NIC<br>on TX | NIC<br>on RX | Parity | | | octet 6b* |
| 0/1<br>ext | connection<br>element | | modem type | | | | | octet 6c* |
| 0/1<br>ext | Other<br>modem type | | Fixed network user rate | | | | | octet 6d* |
| 0/1<br>ext | Acceptable<br>channel<br>codings | | | | Maximum number of<br>traffic channels | | | octet 6e* |
| 0/1<br>ext | UIMI | | | Wanted air interface<br>user rate | | | | octet 6f* |
| 1<br>ext | Acceptable<br>channel codings<br>extended | | | Asymmetry<br>Indication | | 0 0<br>Spare | | octet 6g* |
| 1<br>ext | 1 0<br>layer 2 id. | | User information<br>layer 2 protocol | | | | | octet 7* |

**Figure 10.5.88/3GPP TS 24.008 Bearer capability information element**

NOTE 1: The coding of the octets of the bearer capability information element is not conforming to ITU Q.931.

An MS shall encode the Bearer Capability infomation element according to A/Gb mode call control requirements also if it is requesting for a service in Iu mode, with the following exceptions:

1. A mobile station not supporting A/Gb mode and GERAN Iu mode for the requested bearer service shall set the following parameters to the value "0":

- Maximum number of traffic channels (octet 6e, bits 1-3)
- Acceptable Channel coding(s) (octet 6e, bits 4, 5 and 7)

2. Furthermore, a mobile station not supporting A/Gb mode and GERAN Iu mode for the requested bearer service shall also set the following parameters to the value "0", if the respective octets have to be included in the bearer capability information element according to subclause 10.5.4.5.1 and 3GPP TS 27.001 [36]:
   - UIMI, User initiated modification indication (octet 6f, bits 5-7)
   - Acceptable Channel Codings extended (octet 6g, bits 5-7)

For UTRAN Iu mode the following parameters are irrelevant for specifying the radio access bearer, because multiple traffic channels (multislot) are not deployed, see 3GPP TS 23.034 [104]. However, the parameters if received, shall be stored in the MSC, and used for handover to A/Gb or GERAN Iu mode:

- Maximum number of traffic channels (octet 6e, bits 1-3)
- Acceptable Channel coding(s) (octet 6e, bits 4, 5 and 7)
- UIMI, User initiated modification indication (octet 6f, bits 5-7)
- Acceptable Channel Codings extended (octet 6g, bits 5-7)

NOTE 2: The following parameters are relevant in UTRAN Iu mode for non transparent data calls for deciding which RLP version to negotiate in order to avoid renegotiation of RLP version in case of inter-system handover from UTRAN Iu mode to A/Gb or GERAN Iu mode, see 3GPP TS 24.022 [9]:

- Maximum number of traffic channels (octet 6e, bits 1-3)
- Wanted air interface user rate (octet 6f, bits 1- 4)
- UIMI, User initiated modification indication (octet 6f, bits 5-7).

# 3GPP TSG-CT1 Meeting #38 Tdoc C1-050796
# Cancun, Mexico, 25-29 April 2005

**Title:** **Reply** LS on Service Based Inter-System Handover

**Response to:** LS GP-051179 (C1-050501) on Service Based Inter-System Handover from GERAN2

**Release:** Rel-6

**Work Item:** TEI-6

**Source:** CT1

**To:** GERAN2

**Cc:** TSG SA WG1, TSG SA WG2, TSG CT WG3

**Contact Person:**
**Name:** **Peter Dawes**
**Tel. Number:** +44 7717 275009
**E-mail Address:** peter.dawes@vodafone.com

**Attachments:** CR C1-050795, " Transparent data call request in dual mode case "; CR C1-050741, "Directed Retry Handover for Bearer Service ".

---

## 1. Overall Description:

CT1 thanks GERAN2 for its liaison statement GP-051179 on service based handover. CT1 would like to provide the following answers to the questions raised by GERAN2.

CT1 discussed a possible risk of interoperability issue for a legacy 2G MSCs receiving a SETUP with a Bearer Capability encoded in a way that, until now, has only been used by a UE that accesses a 3G MSC through UTRAN. CT1 considers that encoding by a dual mode MS/UE that accesses a 2G MSC through GERAN is not not an issue as 2G MSCs will reject the call setup, with no adverse consequences.

CT1 also discussed the option of adding a new optional information element of "comprehension required". CT1 decided that because no interoperability issue was identified, a new information element is not needed. CT1 noted that a legacy 2G MSC that is unable to provide the requested bearer can return cause code 65 "bearer service not implemented" to provide a reason for failure to the mobile terminal.

The CRs agreed by CT1 are attached.

## 2. Actions:

**To GERAN2 group.**

**ACTION:**

None.

## 3. Date of Next TSG-CN1 Meetings:

| | | |
|---|---|---|
| CT1_39 | 29th August – 2nd September 2005 | London, UK |
| CT1_40 | 31st October – 4th November 2005 | Berlin, Germany |

## 3GPP TSG-CT1 Meeting #38 Tdoc C1-050797
## Cancun, Mexico, 25-29 April 2005

**Title:** **LS on NAS actions in support of MBMS Reception**

**Response to:** **LS (R2-051109/C1-050503) titled "LS on 'release' of non-prioritised non-MBMS PS services" from RAN2**

**Release:** **Rel-6**

**Work Item:** **MBMS**

**Source:** **CT1**

**To:** **RAN2, SA2, GERAN2**

**Cc:** **RAN3, CT4, SA1**

**Contact Person:**
**Name:** Chen-Ho CHIN
**Tel. Number:** +44-7880-535.108
**E-mail Address:** **chenho.chin@samsung.com**

**Attachments:** None

---

**1. Overall Description:**

CT1 would like to thank RAN2 for their LS (R2-051109/C1-050503). In this LS (R2-051109/C1-050503) RAN2 highlight the problem that "*UE may be unable to receive an MBMS service in conjunction with a non- MBMS services*" for two cases, namely:-

- *when the UE uses dedicated channels i.e. is in CELL_DCH state (support of MBMS service reception is optional in this state).*
- *when the UE is on an MBMS preferred frequency that is congested.*

In the discussion in CT1, CT1 agrees that this is a problem.

During the discussion, CT1 saw a contribution (C1-050509) that elaborates on the problem and suggested some solutions. However, CT1 could not agree on any solution on this and would like to seek guidance from SA2. The reasons why CT1 could not agree to any solution is principally because,

- the possible solutions discussed in the CT1 impacts many WGs, going forward with any solution would require a remit from SA2 to all involved WGs.
- CT1 is of the opinion that any change should propagate from Stage 2 Specifications of MBMS, which too is under the responsibility of SA2.
- it should also be investigated by GERAN2 whether a similar problem applies.
- a problem of the proposed solution of suspending the PS services that are considered of lower priority than MBMS reception is the additional signalling that this will create, especially if there are a lot of users in a cell.

CT1 would further like to indicate to SA2 that this problem has arisen quite late and is not in the Exception List of outstanding work for MBMS submitted at last CN Plenary (NP#27). Therefore, it is not clear to CN1 whether this is a Rel-6 issue – and thus has to be solved as an essential correction - or Rel-7 issue

In RAN2's LS (R2-051109/C1-050503), RAN2 also ask the following question to CT1.

> "*RAN2 would like to understand if the disruption in the MBMS service reception when maintaining the separate PDP context for IMS signalling is considered acceptable*"

CT1 has discussed this and agrees that IMS Signalling should be allowed to continue during MBMS reception. With respect to that, CT1 would like RAN2 to note that whilst the expectations are that IMS Signalling will be supported through a PDP Context established for IMS Signalling, it is possible that some users do set up a general purpose PDP Context for IMS Signalling

## 2. Actions:

**To SA2 group.**

**ACTION:** CT1 kindly requests SA2 to address this problem and provide a way forward for all the appropriate Stage 3 Specifications.

**To GERAN2 group.**

**ACTION:** CT1 kindly request GERAN2 to investigate whether a similar problem as the one raised by RAN2 might also arise when MBMS is used in A/Gb mode.

## 3. Date of Next TSG-CN1 Meetings:

| | | |
|---|---|---|
| CT1_39 | 29th August – 2nd September 2005 | London, UK |
| CT1_40 | 31st October – 4th November 2005 | Berlin, Germany |

# 3GPP TSG-CT1 Meeting #38 Tdoc C1-050798
# Cancun, Mexico, 25-29 April 2005

|  |  |
|---|---|
| **Title:** | Reply LS on Support of DSAC and Network sharing in Rel-5 UEs as optional features |
| **Response to:** | LS (C1-050504) on optional support of DSAC and Network sharing in Rel-5 UEs from RAN2 |
| **Release:** | Rel-6 |
| **Work Item:** | ACBOP/ NTShar |
|  |  |
| **Source:** | 3GPP WG CT1 |
| **To:** | SA, RAN2 |
| **CC:** | RAN, CT |

**Contact Person:**

|  |  |
|---|---|
| **Name:** | Yosuke Hayashi |
| **Tel. Number:** | +81 46 840 3370 |
| **E-mail Address:** | hayashiyo@nim.yrp.nttdocomo.co.jp |

**Attachments:**

---

## 1. Overall Description:

CT1 thanks RAN2 for their liaison statement (C1-050504) on optional support of DSAC and Network sharing in Rel-5 UEs. CT1 was asked to investigate into any technical issues in implementing these Rel-6 features in Rel-5 UEs and comment on how to document early implementation of these features in 3GPP specifications if they are seen as optional candidate features for earlier releases.

During the discussion, some strong concerns were raised against the principle of allowing early implementation of features that are not national regulatory requirements, and in particular when the relevant Work Items do not reflect such agreements. As such, CT1 could not make a unanimous recommendation on supporting the principle itself. There were no immediate technical issues being raised in implementing DSAC and/or Network Sharing in Rel-5 UEs, but CT1 believes that, if early implementations are allowed, such candidate features should be independent of each other and from other features in the same release, and so further investigations are needed in this respect.

Despite the fact that CT1 could not reach a common decision on the early implementation principle, CT1 discussed how candidate features for early implementation such as DSAC and Network Sharing could be documented if the whole principle was allowed. CT1 agreed that frozen releases shall not be changed due to features that could be implemented in earlier releases. It was seen not feasible to document such features in the existing Technical Specifications, but a Technical Report for each feature could be considered instead, if the principle was agreed.

## 2. Actions:

**To SA plenary.**

**ACTION:** CT1 kindly asks SA plenary whether DSAC and/or Network Sharing are possible candidates for early implementation and provide guidance on the principle and how to proceed with early implementation.

**To RAN2 group.**

**ACTION:** CT1 kindly asks RAN2 to take these answers into account when investigating further on early implementation of DSAC and Network Sharing.

## 3. Date of Next TSG-CN1 Meetings:

| | | |
|---|---|---|
| CT1_39 | 29th August – 2nd September 2005 | London, UK |

**3GPP TSG-CT1 Meeting #38** **Tdoc C1-050799**
**Cancun, Mexico, 25-29 April 2005**

| | |
|---|---|
| **Title:** | Reply LS on GPRS P-CSCF discovery procedure |
| **Response to:** | LS (S2-050959/C1-050589) on LS on GPRS P-CSCF discovery procedure |
| **Release:** | Rel-5 , Rel-6 |
| **Work Item:** | IMS-CCR , IMS2 |

| | |
|---|---|
| **Source:** | CT1 |
| **To:** | SA2 |
| **Cc:** | CT3 |

**Contact Person:**

| | |
|---|---|
| **Name:** | Atle Monrad |
| **Tel. Number:** | +47 454 10 665 |
| **E-mail Address:** | atle.monrad@ericsson.com |

**Attachments:** C1-050673 (Rel-5) and C1-050674 (rel-6)

### 1. Overall Description:

CT1 thanks SA2 for the LS.

The subject was thoroughly discussed in CT1 #38 and the following conclusions were reached:

- CT1 agreed that usage of the default port (5060) as recommended in RFC 3261 should be mandated. Due to this, CT1 has agreed CRs from Rel-5 and onwards to clarify this.
- With respect to the "GPRS procedure for P-CSCF discovery", CT1 can confirm that it will not be possible to perform initial REGISTER requests towards other ports than the default port.

  CT1 could not agree on CRs that would enhance the "GPRS procedure for P-CSCF discovery" to include port information. Consequently, if the UE decides to use GPRS procedures, the default port (5060) has to be used.

### 2. Actions:

**To SA2 group.**

**ACTION:**

To take the reply from CT1 into account and possibly guide CT1 further on the subject.

### 3. Date of Next TSG-CN1 Meetings:

| | | |
|---|---|---|
| CT1_39 | 29th August – 2nd September 2005 | London, UK |

# 3GPP TSG-CT1 Meeting #38 Tdoc C1-050805
# Cancun, Mexico, 25-29 April 2005

| | |
|---|---|
| **Title:** | Reply LS on IOT test for the feature 'Combinational Services' |
| **Response to:** | |
| **Release:** | Rel-7 |
| **Work Item:** | CSICS |
| | |
| **Source:** | CT1 |
| **To:** | CT, RAN |
| **Cc:** | SA |

**Contact Person:**

| | |
|---|---|
| **Name:** | Atle Monrad |
| **Tel. Number:** | +47 454 10 665 |
| **E-mail Address:** | atle.monrad@ericsson.com |

**Attachments:** None

## 1. Overall Description:

The feature 'combinational services' has WIDs and TSs for stage 1 and stage 2. CT1 is further proposing a new TR to take stage 3 aspects of the feature into account. The feature addresses two main capabilities:

- Combining CS and IMS services
- Terminal/Radio Capability detection

To introduce interoperability test (IOT) under the scope of CT was briefly discussed at CN plenary #26, and the following conclusion was minuted when the ToR for CT was discussed:

*"it was clarified that the current ToR does not preclude interoperability testing and CN would consider WIDs on this topic when they are available".*

A work item was proposed to introduce a new TS for interoperability testing in CT1. However, CT1 could not agree to this WID and would like to get feedback and guidance on how to proceed on the topic.

CT1 is aware that work is proposed to do conformance testing in RAN of IMS and that this must be taken into account when deciding how and where to progress this work.

## 2. Actions:

**To CT and RAN groups.**

**ACTION:**

CT1 kindly asks the CT and RAN groups the following:

- If interoperability test is needed
- How such testing should be done
- Where such testing should be performed

## 3. Date of Next TSG-CT1 Meetings:

| | | |
|---|---|---|
| CT1_39 | 29th August – 2nd September 2005 | London, UK |

**3GPP TSG-CT1 Meeting #38** **Tdoc C1-050806**
**Cancun, Mexico, 25-29 April 2005**

| | |
|---|---|
| **Title:** | Reply LS on "misalignment between TS 33.220 and TS 24.109" |
| **Response to:** | LS (C1-050734) on "misalignment between TS 33.220 and TS 24.109" from SA3 |
| **Release:** | Rel-6 |
| **Work Item:** | SEC1-SC |
| **Source:** | CT1 |
| **To:** | SA3 |
| **Cc:** | |

**Contact Person:**

**Name:** Varga József
**Tel. Number:** +36209849040
**E-mail Address:** jozsef.varga@nokia.com

**Attachments:** CT1 CR "Alignment with TS 33.220" for TS 24.109
(C1-050807_24109CR017r1_alignment.zip)

---

### 1. Overall Description:

CT1 thanks SA3 for their LS on misalignment between TS 33.220 and TS 24.109.

Enclosed please find the CR, agreed by CT1, aligning TS 24.109 with TS 33.220 according to your request.

### 2. Actions:

**To SA3 group.**

**ACTION:** CT1 kindly asks SA3 to note the above answer from CT1.

### 3. Date of next CT1 meetings:

| | | |
|---|---|---|
| CT1_38 | 25th -29th April 2005 | Cancun, Mexico |
| CT1_39 | 29th August – 2nd September 2005 | London, UK |

3GPP TSG-CT1 #38 *C1-050807*
Cancun, Mexico, 25-29 April 2005

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.109** | **CR** | **17** | ⌘**rev** | **1** | ⌘ | Current version: | **6.2.0** | ⌘ |

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

***Proposed change affects:*** UICC apps⌘ ☒ ME ☐ Radio Access Network ☐ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Usage of Ks_int_NAF | | |
| ***Source:*** | ⌘ | Axalto, Gemplus | | |
| ***Work item code:*** | ⌘ | SEC1-SC | ***Date:*** ⌘ | 29/04/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |

| | |
|---|---|
| *Use one of the following categories:* | *Use one of the following releases:* |
| ***F*** *(correction)* | *2 (GSM Phase 2)* |
| ***A*** *(corresponds to a correction in an earlier release)* | *R96 (Release 1996)* |
| ***B*** *(addition of feature),* | *R97 (Release 1997)* |
| ***C*** *(functional modification of feature)* | *R98 (Release 1998)* |
| ***D*** *(editorial modification)* | *R99 (Release 1999)* |
| Detailed explanations of the above categories can | *Rel-4 (Release 4)* |
| be found in 3GPP TR 21.900. | *Rel-5 (Release 5)* |
| | *Rel-6 (Release 6)* |
| | *Rel-7 (Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | SA3 has identified a misallignement between TS 33.220 and TS 24.109 in TD S3-050289. |
| ***Summary of change:*** | ⌘ | Update TS 24.109 to mention explicitly that the usage of Ks_int_NAF is possible. |
| ***Consequences if not approved:*** | ⌘ | Misallignement between TS 33.220 and TS 24.109 |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.1 | | | |
| | | **Y** | **N** | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ |
| | | | **X** | Test specifications | |
| | | | **X** | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | | |

## How to create CRs using this form:

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text.  Delete those parts of the specification which are not relevant to the change request.

## 5.1 Introduction

The usage of bootstrapped security association i.e. B-TID and Ks_NAF (or Ks_ext_NAF or Ks_int_NAF) over Ua interface depends on the application protocol used between UE and NAF.

The Ua interface is used to supply the B-TID, generated during the bootstrapping procedure, to the network application function (NAF), and Zn interface is used by the NAF to retrieve the Ks_NAF or Ks_ext_NAF or Ks_int_NAF from BSF. The default is the use of Ks_(ext)_NAF, but the usage of Ks_int_NAF in Ua interface is possible. The Ua interface depends on type of NAF. The Zn interface is defined in 3GPP TS 29.109 [3]. This clause describes how B-TID and Ks_NAF or Ks_ext_NAF can be utilized ~~in general Ua usage~~, as specified in 3GPP TS 33.220 [1], and in the context of more specific Ua usage, as specified for deployment of HTTPS in 3GPP TS 33.222 [4A], or for a PKI portal in 3GPP TS 33.221 [4]).