3GPP TSG CN Meeting #27 **NP-050060**
9th - 11th March 2005. Tokyo, Japan.

Source: CN1

Title: Liaison Statements sent from CN1 since CN#26

Agenda item: 6.1.1

Document for: INFORMATION

The document contains all LSs that have been agreed in CN1 since TSG CN#26.

TDoc #	Tdoc Title	Status
N1-050206	Reply LS (to R2-050272) on AS-NAS interaction for MBMS	To: RAN2, SA2;CC: GERAN2, RAN3
N1-050270	Misalignment amongst the 3GPP specifications, “Re-authentication and key set change during inter-system handover”	To: SA; CC:SA3, CN, RAN, RAN3, RAN2
N1-050271	Reply LS (to R3-041648) on MBMS Information Elements over Iu interface	To: RAN3; CC:GERAN2, SA2, SA4, CN3, CN4, RAN2
N1-050272	Reply LS to SA2 on 3rd party registration and shared public user identities	To: SA2
N1-050273	Reply LS on "S-CSCF client address comparisons and their affect on de-registrations"	To: CN4
N1-050276	LS on PS handover and Robust Header Compression (RoHC) Context Relocation	To: RAN2; CC:GERAN2, SA2, RAN3, CN4
N1-050277	Reply LS on IP multimedia messaging capabilities	To: SA1; CC: CN
N1-050278	LS on provisioning of the UE RAC and START_PS to the network	To: GERAN2, RAN2, RAN3
N1-050279	Reply LS on "Misalignment between VGCS stage 1 and 2"	To: SA1
N1-050371	Reply LS on Application Charging ID	To: SA5; CC:SA2
N1-050376	Alignment of specifications between CN1 and SA3 with respect to fallback to full authentication	To: SA3
N1-050383	Reply LS to SA2 on transport of HSS address	To: CN4
N1-050406	Reply LS (to G2-0402911) on the PS Handover Work	To: GERAN; CC:SA2, RAN2, RAN3, CN4
N1-050407	Reply LS (to R2-042734 and S2-050488) on NAS signalling load at MBMS Session Start/Stop	To: RAN2; CC:SA1, SA2, RAN3, GERAN2
N1-050408	LS to SA3 with comments and proposed changes to TR 33.878	To: SA3
N1-050410	LS on service based inter-system hand over	To: SA1, SA2, GERAN2; CC:CN3
N1-050415	Reply LS on LS on protocol aspects for CSI	To: SA2
N1-050416	LS on status of 3GPP IMS management object	To: OMA PAG, OMA POC, OMA DM, 3GPP2 TSG-X; CC: CN

3GPP TS 24.167 V2.0.0 (2005-02)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network; 3GPP IMS Management Object (MO); Stage 3 (Release 6)

Keywords
UMTS, IMS, SIP, Multimedia, Management

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This document defines a mobile device 3GPP IMS Management Object. The management object is compatible with OMA Device Management protocol specifications, version 1.1.2 and upwards, and is defined using the OMA DM Device Description Framework as described in OMA-SyncML-DMTND-V1-1 [6] and OMA-SyncML-DMStdObj-V1-1-2 [7].

The 3GPP IMS Management Object consists of relevant parameters that can be managed for the IM CN Subsystem. This includes the basic framework defined in 3GPP TS 23.228 [4] and 3GPP TS 24.229 [5], and early IMS as defined in 3GPP TS 23.221 [3].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the 3GPP IMS Management Object 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 23.003: "Numbering, addressing and identification".

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

[4] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[5] 3GPP TS 24.229: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[6] OMA-SyncML-DMTND-V1-1: "SyncML Device Management Tree and Description".

[7] OMA-SyncML-DMStdObj-V1-1-2: "SyncML Device Management Standardized Objects".

[8] RFC 1123: "Requirements for Internet Hosts -- Application and Support".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

CN	Core Network
CSCF	Call Session Control Function
DDF	Device Description Framework
DM	Device Management
IMS	IP Multimedia core network Subsystem

IP	Internet Protocol
MO	Management Object
OMA	Open Mobile Alliance
P-CSCF	Proxy – CSCF
PDP	Packet Data Protocol
SIP	Session Initiation Protocol
UE	User Equipment

4 3GPP IMS Management Object

The 3GPP IMS Management Object is used to manage settings of the UE for IM CN Subsystem protocols. The Management Object covers generic parameters for the IM CN subsystem. The Management Object enables the management of the settings on behalf of the end user.

The Management Object Identifier is: org.3gpp/1.0/SIPCore

Protocol compatibility: This MO is compatible with OMA DM 1.2.

Management object name: 3GPP_IMS

Editor's Note: The name of the management object to be determined by OMA.

The following nodes and leaf objects are possible under the 3GPP_IMS node:

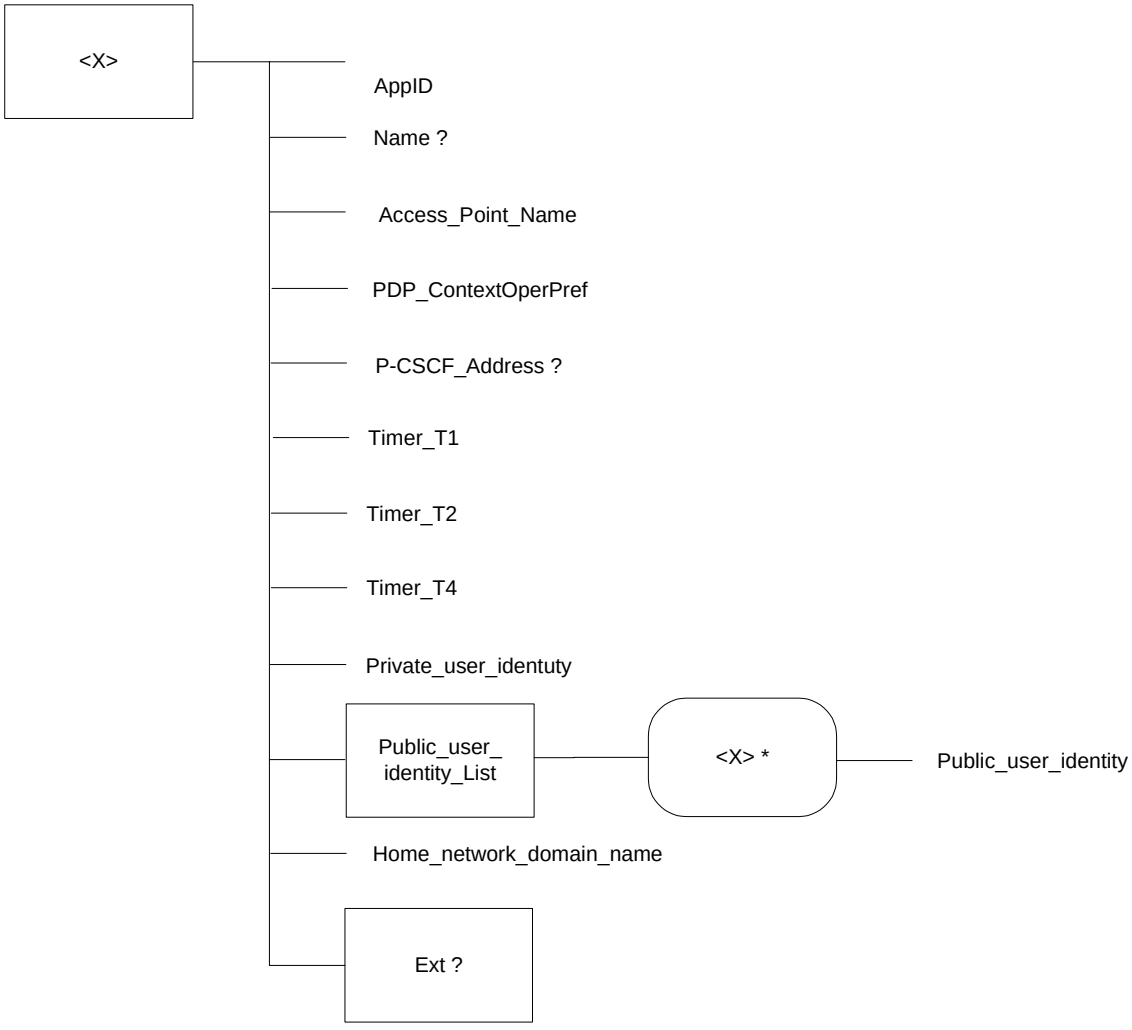

Figure 1: The 3GPP IMS Management Object

5 Management Object parameters

5.1 General

This clause describes the parameters for the 3GPP IMS Management Object.

5.2 Node: /<X>

This interior node acts as a placeholder for one or more accounts for a fixed node.

- Occurrence: OneOrMore
- Format: node
- Access Types: Get
- Values: N/A

The interior node is mandatory if the UE supports the IM CN Subsystem. Support for a UE is defined by the user agent role as defined in 3GPP TS 24.229 [5].

5.3 /<X>/AppID

The AppID identifies the type of the application service available at the described application service access point. The value is expected to be globally unique.

- Occurrence: One
- Format: chr
- Access Types: Get
- Values: <Globally unique value>

Editor's Note: The value of the 3GPP_IMS/AppID to be determined by OMA

5.4 /<X>/Name

The Name leaf is a name for the 3GPP_IMS settings.

- Occurrence: ZeroOrOne
- Format: chr
- Access Types: Get
- Values: <User displayable name>

5.5 /<X>/Access_Point_Name

The Access_Point_Name leaf defines the APN to use for where the PDP context for the SIP towards the FQDN to a P-CSCF.

- Occurrence: One
- Format: chr
- Access Types: Get, Replace
- Values: <The IMS access point name>

The format of the APN is defined by 3GPP TS 23.003 [2].

Example: operator.com

5.6 /<X>/PDP_ContextOperPref

The PDP_ContextOperPref leaf indicates an operator's preference to have a dedicated PDP context for SIP signalling.

- Occurrence: One
- Format: bin
- Access Types: Get, Replace
- Values: 0, 1
  0 – Indicates that the operator has no preference for a dedicated PDP context for SIP signalling.
  1 – Indicates that the operator has preference for a dedicated PDP context for SIP signalling.

The PDP_ContextOperPref leaf indicates a preference only. 3GPP TS 24.229 [5] describes the normative options and the procedures for establishment of a dedicated PDP context for SIP signalling.

5.7 /<X>/P-CSCF_Address

The P-CSCF_Address leaf defines an FQDN to an IPv4 P-CSCF.

- Occurrence: ZeroOrOne
- Format: chr
- Access Types: Get, Replace
- Values: <A fully qualified domain name>

The P-CSCF_Address leaf shall only be used in early IMS implementations as described in 3GPP TS 23.221 [3].

The FQDN, or domain name as defined by RFC 1123 [8], is represented as character-labels with dots as delimiters.

Example: operator.com

5.8 /<X>/Timer_T1

The Timer_T1 leaf defines the SIP timer T1 – the RTT estimate.

- Occurrence: One
- Format: chr
- Access Types: Get, Replace
- Values: <The round trip time>

The Timer_T1 leaf is an estimate for the round trip time in the system (UE – P-CSCF). The timer value shall be given in milliseconds. The recommended value is defined in 3GPP TS 24.229 [5].

Example: 2000 (milliseconds)

5.9 /<X>/Timer_T2

The Timer_T2 leaf defines the SIP timer T2 – the maximum retransmit interval for non-INVITE requests and INVITE responses.

- Occurrence: One
- Format: chr
- Access Types: Get, Replace
- Values: < The maximum retransmit interval for non-INVITE requests and INVITE responses>

The Timer_T2 leaf is an estimate for the maximum retransmit interval for non-INVITE requests and INVITE responses. The timer value shall be given in milliseconds. The recommended value is defined in 3GPP TS 24.229 [5].

Example: 16000 (milliseconds)

5.10 /<X>/Timer_T4

The Timer_T4 leaf defines the SIP timer T4 – the maximum duration a message will remain in the network.

- Occurrence: One

- Format: chr
- Access Types: Get, Replace
- Values: <The maximum duration a message will remain in the network>

The Timer_T4 leaf is an estimate for the maximum duration a message will remain in the network. The timer value shall be given in milliseconds. The recommended value is defined in 3GPP TS 24.229 [5].

Example: 17000 (milliseconds)

5.11 /<X>/Private_user_identity

The Private_user_identity leaf represents the private user identity.

- Occurrence: One
- Format: chr
- Access Types: Get
- Values: <A private user identity>

NOTE: The Private_user_identity leaf value is populated by the UE using the procedures to obtain the private user identity specified in 3GPP TS 24.229 [5].

The format of the private user identity is defined by 3GPP TS 23.003 [2].

Example: 234150999999999@ims.mnc015.mcc234.3gppnetwork.org

5.12 /<X>/Public_user_identity_List/

The Public_user_identity_List interior node is used to allow a reference to a list of public user identities.

- Occurrence: One
- Format: node
- Access Types: Get
- Values: N/A

5.13 /<X>/Public_user_identity_List/<X>

This run-time node acts as a placeholder for one or more public user identities.

- Occurrence: OneOrMore
- Format: node
- Access Types: Get
- Values: N/A

5.14 /<X>/Public_user_identity_List/<X>/Public_user_identity

The Public_user_identity leaf represents one or more public user identities.

- Occurrence: One
- Format: chr
- Access Types: Get
- Values: <A public user identity>

NOTE: The Public_user_identity leaf value is populated by the UE using the procedures to obtain the public user identity specified in 3GPP TS 24.229 [5].

The temporary public user identity if derived is populated and stored as the topmost element in the Public_user_identity_List as specified in 3GPP TS 24.229 [5].

The format of the public user identity is defined by 3GPP TS 23.003 [2].

Example: sip: sip:user@domain

5.15 /<X>/Home_network_domain_name

The Home_network_domain_name leaf indicates the operator's home network domain.

- Occurrence: One
- Format: chr
- Access Types: Get
- Values: <The home network domain name>

NOTE: The Home_network_domain_name leaf value is populated by the UE using the procedures to obtain the home network domain name specified in 3GPP TS 24.229 [5].

The format of the home network domain name is defined by 3GPP TS 23.003 [2].

Example: ims.mnc015.mcc234.3gppnetwork.org

5.16 /<X>/Ext/

The Ext is an interior node for where the vendor specific information about the 3GPP-IMS MO is being placed (vendor meaning application vendor, device vendor etc.). Usually the vendor extension is identified by vendor specific name under the ext node. The tree structure under the vendor identified is not defined and can therefore include un-standardized sub-tree.

- Occurrence: ZeroOrOne
- Format: node
- Access Types: Get
- Values: N/A

Annex A (informative): Management Object DDF

This DDF is the standardized minimal set. A vendor can define it's own DDF for the complete device. This DDF can include more features than this minimal standardized version.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE MgmtTree PUBLIC "-//OMA//DTD SYNCML-DMDDF 1.2//EN"
http://www.openmobilealliance.org/tech/DTD/OMA-SyncML-DMDDF-1_2.dtd>

<MgmtTree>
    <VerDTD>1.2</VerDTD>
    <Man>--The device manufacturer--</Man>
    <Mod>--The device model--</Mod>

    <Node>
        <NodeName>3GPP_IMS</NodeName>
        <DFProperties>
            <AccessType>
                <Get/>
            </AccessType>
            <Description>3GPP IMS settings</Description>
            <DFFormat>
                <node/>
            </DFFormat>
            <Occurrence>
                <OneOrMore/>
            </Occurrence>
            <Scope>
                <Permanent/>
            </Scope>
            <DFTitle>The 3GPP IMS Management Object.</DFTitle>
            <DFType>
                <DDFName/>
            </DFType>
        </DFProperties>

        <Node>
            <NodeName>AppID</NodeName>
            <DFProperties>
                <AccessType>
                    <Get/>
                </AccessType>
                <DFFormat>
                    <chr/>
                </DFFormat>
                <Occurrence>
                    <One/>
                </Occurrence>
                <Scope>
                    <Permanent/>
                </Scope>
                <DFTitle>The Application ID.</DFTitle>
                <DFType>
                    <MIME>text/plain</MIME>
                </DFType>
            </DFProperties>
        </Node>

        <Node>
            <NodeName>Name</NodeName>
```

```
            <DFProperties>
                <AccessType>
                    <Get/>
                </AccessType>
                <DFFormat>
                    <chr/>
                </DFFormat>
                <Occurrence>
                    <ZeroOrOne/>
                </Occurrence>
                <Scope>
                    <Dynamic/>
                </Scope>
                <DFTitle>User displayable name for the node.</DFTitle>
                <DFType>
                    <MIME>text/plain</MIME>
                </DFType>
            </DFProperties>
        </Node>

        <Node>
            <NodeName>Access_Point_Name</NodeName>
            <DFProperties>
                <AccessType>
                    <Get/>
                    <Replace/>
                </AccessType>
                <DFFormat>
                    <chr/>
                </DFFormat>
                <Occurrence>
                    <One/>
                </Occurrence>
                <Scope>
                    <Permanent/>
                </Scope>
                <DFTitle>The IMS access point name.</DFTitle>
                <DFType>
                    <MIME>text/plain</MIME>
                </DFType>
            </DFProperties>
        </Node>

        <Node>
            <NodeName>PDP_ContextOperPref</NodeName>
            <DFProperties>
                <AccessType>
                    <Get/>
                    <Replace/>
                </AccessType>
                <DFFormat>
                    <bin/>
                </DFFormat>
                <Occurrence>
                    <One/>
                </Occurrence>
                <Scope>
                    <Permanent/>
                </Scope>
                <DFTitle>Indication of the operator's preference for a dedicated PDP context for IMS
signalling.</DFTitle>
                <DFType>
                    <MIME>text/plain</MIME>
```

```
            </DFType>
        </DFProperties>
    </Node>

    <Node>
        <NodeName>P-CSCF_Address</NodeName>
        <DFProperties>
            <AccessType>
                <Get/>
                <Replace/>
            </AccessType>
            <DFFormat>
                <chr/>
            </DFFormat>
            <Occurrence>
                <ZeroOrOne/>
            </Occurrence>
            <Scope>
                <Dynamic/>
            </Scope>
            <DFTitle>The address of the P-CSCF.</DFTitle>
            <DFType>
                <MIME>text/plain</MIME>
            </DFType>
        </DFProperties>
    </Node>

    <Node>
        <NodeName>Timer_T1</NodeName>
        <DFProperties>
            <AccessType>
                <Get/>
                <Replace/>
            </AccessType>
            <DFFormat>
                <chr/>
            </DFFormat>
            <Occurrence>
                <One/>
            </Occurrence>
            <Scope>
                <Permanent/>
            </Scope>
            <DFTitle>RFC 3261, timer T1.</DFTitle>
            <DFType>
                <MIME>text/plain</MIME>
            </DFType>
        </DFProperties>
    </Node>

    <Node>
        <NodeName>Timer_T2</NodeName>
        <DFProperties>
            <AccessType>
                <Get/>
                <Replace/>
            </AccessType>
            <DFFormat>
                <chr/>
            </DFFormat>
            <Occurrence>
                <One/>
            </Occurrence>
```

```
            <Scope>
                <Permanent/>
            </Scope>
            <DFTitle>RFC 3261, timer T2.</DFTitle>
            <DFType>
                <MIME>text/plain</MIME>
            </DFType>
        </DFProperties>
    </Node>

    <Node>
        <NodeName>Timer_T4</NodeName>
        <DFProperties>
            <AccessType>
                <Get/>
                <Replace/>
            </AccessType>
            <DFFormat>
                <chr/>
            </DFFormat>
            <Occurrence>
                <One/>
            </Occurrence>
            <Scope>
                <Permanent/>
            </Scope>
            <DFTitle>RFC 3261, timer T4.</DFTitle>
            <DFType>
                <MIME>text/plain</MIME>
            </DFType>
        </DFProperties>
    </Node>

    <Node>
        <NodeName>Private_user_identity</NodeName>
        <DFProperties>
            <AccessType>
                <Get/>
            </AccessType>
            <DFFormat>
                <chr/>
            </DFFormat>
            <Occurrence>
                <One/>
            </Occurrence>
            <Scope>
                <Permanent/>
            </Scope>
            <DFTitle>The private user identity.</DFTitle>
            <DFType>
                <MIME>text/plain</MIME>
            </DFType>
        </DFProperties>
    </Node>

    <Node>
        <NodeName>Public_user_identity_List</NodeName>
        <!-- The Public_user_identity_List node starts here. -->
        <DFProperties>
            <AccessType>
                <Get/>
            </AccessType>
            <DFFormat>
```

```
                <node/>
            </DFFormat>
            <Occurrence>
                <One/>
            </Occurrence>
            <Scope>
                <Permanent/>
            </Scope>
            <DFTitle>A collection of public user identity objects.</DFTitle>
            <DFType>
                <DDFName/>
            </DFType>
        </DFProperties>
        <Node>
            <NodeName/>
            <DFProperties>
                <AccessType>
                    <Get/>
                </AccessType>
                <DFFormat>
                    <node/>
                </DFFormat>
                <Occurrence>
                    <OneOrMore/>
                </Occurrence>
                <Scope>
                    <Dynamic/>
                </Scope>
                <DFTitle>The "name" node for a public user identity object.</DFTitle>
                <DFType>
                    <DDFName/>
                </DFType>
            </DFProperties>
            <Node>
                <NodeName>Public_user_identity</NodeName>
                <DFProperties>
                    <AccessType>
                        <Get/>
                    </AccessType>
                    <DFFormat>
                        <chr/>
                    </DFFormat>
                    <Occurrence>
                        <One/>
                    </Occurrence>
                    <Scope>
                        <Permanent/>
                    </Scope>
                    <DFTitle>The public user identity.</DFTitle>
                    <DFType>
                        <MIME>text/plain</MIME>
                    </DFType>
                </DFProperties>
            </Node>
        </Node>
    </Node>

    <Node>
        <NodeName>Home_network_domain_name</NodeName>
        <DFProperties>
            <AccessType>
                <Get/>
```

```
            </AccessType>
            <DFFormat>
                <chr/>
            </DFFormat>
            <Occurrence>
                <One/>
            </Occurrence>
            <Scope>
                <Permanent/>
            </Scope>
            <DFTitle>The home network domain name.</DFTitle>
            <DFType>
                <MIME>text/plain</MIME>
            </DFType>
        </DFProperties>
    </Node>

    <Node>
        <NodeName>Ext</NodeName>
        <!-- The Extension node starts here. -->
        <DFProperties>
            <AccessType>
                <Get/>
                <Replace/>
            </AccessType>
            <DFFormat>
                <node/>
            </DFFormat>
            <Occurrence>
                <ZeroOrOne/>
            </Occurrence>
            <Scope>
                <Dynamic/>
            </Scope>
            <DFTitle>A collection of all Extension objects.</DFTitle>
            <DFType>
                <DDFName/>
            </DFType>
        </DFProperties>
    </Node>

</Node>

</MgmtTree>
```

Annex B (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2004-10					Version 0.0.1: Preliminary proposal		0.0.1	
2004-11					Version 0.0.2: Version after CN1 #36	0.0.1	0.0.2	
2004-12					Version 1.0.0: Version after CN1#36 and editorial corrections	0.0.2	1.0.0	
2005-02					Version 1.1.0: Version after CN1#37 and editorial corrections	1.0.0	1.1.0	N1-050330 N1-050393
2005-02					Version 2.0.0 created by MCC	1.1.0	2.0.0	

3GPP TSG-CN1 Meeting #37 Tdoc N1-050206
Sydney, Australia, 14-18 February 2005

Title: Reply LS (to R2-050272) on AS-NAS interaction for MBMS

Response to: LS (N1-050032/R2-050272) on “Reply LS (to N1-041944) on AS-NAS interaction for MBMS

Release: Rel-6

Work Item: MBMS

Source: CN1

To: RAN2, SA2

Cc: GERAN2, RAN3

Contact Person:
Name: Christian Herrero
Tel. Number: +46 46231812
E-mail Address: christian.Herrero@ericsson.com

Attachments: None

---

1. Overall Description:

CN1 would like to inform RAN2 that a CR has been agreed at CN1#37 which introduces the mapping of the appropriate NAS procedure (i.e. Service request with type “MBMS notification response”) to RRC establishment cause. Therefore, TS 24.008 is updated in the Annex L to reflect the mapping of this NAS procedure. This allows the network (RAN) to record the attempts of the NAS procedure Service request with service type “MBMS notification response” initiated by the UE.

Regarding the MBMS bearer capabilities and its usage, CN1 would to bring to the attention of RAN2 that the MBMS bearer capabilities was specified by SA2 in TS 23.246. Afterwards, CN1 was requested to include the MBMS bearer capability and its usage into CN1 specifications (i.e. TS 24.008). Therefore, what CN1 has specified is the mechanism at core network protocols for the UE to inform the SGSN about its MBMS bearer capabilities during the MBMS Multicast service activation procedure.

It’s CN1 understanding that the MBMS bearer capabilities is not directly related to the AS of the UE and its radio access capabilities in one specific radio access technology (e.g. UMTS), but more related to higher layer capabilities in the UE to receive MBMS data (maximum bit rate for downlink). However, CN1 would like to invite SA2 to clarify the MBMS bearer capabilities and its need and usage to both RAN2 and CN1 taking into the account the concerns raised by RAN2, as follows:

> In particular, RAN2 does not understand what is intended by 'static physical capabilities'. RAN1 and RAN2 are defining minimum UE radio access capabilities that are required to be supported by all UEs that are capable of MBMS. These include a number of detailed layer 1 parameters that are not easy to convert into a single 'maximum UE bit rate capability'. The minimum capabilities define configuration constraints for the channels used to deliver MBMS - i.e. as long as the channel configuration chosen by the network is within these constraints then it will be possible for any MBMS capable UE, that is not attempting to receive another service in parallel, to receive an MBMS service sent on this channel. It is envisaged that some UEs may support more than the minimum capability, for example to be able to receive multiple services in parallel. It is not envisaged by RAN1 or RAN2 that some UEs will support more than the minimum capability for the purpose of receiving higher data rate MBMS services.
>
> In addition RAN2 does not understand how a single value of 'maximum UE bit rate capability' can be applicable to both UMTS and GSM radio access technologies.

2. Actions:

To SA2 group.

ACTION: CN1 kindly requests SA2 to provide further information on the use of the MBMS bearer capability and its purpose to both CN1 and RAN2.

3. Date of Next TSG-CN1 Meetings:

CN1_37	14th – 18th February 2005	Sydney, Australia
CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050270
Sydney, Australia, 14-18 February 2005

Title: Misalignment amongst the 3GPP specifications, "Re-authentication and key set change during inter-system handover"

Response to: R2-042611
Work Item: TEI-5

Source: CN1
To: SA
Cc: SA3, CN, RAN, RAN3, RAN2

Contact Person:
Name: Rouzbeh Farhoumand
Tel. Number: +1 469 682 9924
E-mail Address: rouzbeh.farhoumand@ericsson.com

Attachments: None

---

1. Overall Description:

A year ago, at CN1#33 meeting in February 2004, a misalignment amongst the 3GPP specifications on handling of key sets from R99 between the terminal and the network was identified. At that meeting, CN1 concluded that the inter-system handover from GERAN to UMTS procedures after re-authentication (i.e. 'late AKA') would always fail, if the handover occurred before the new keys were taken into use. Since CN1 was of the opinion that a re-authentication in the CS domain may be a rare event in R99 and also to avoid creating problems for the existing R99 mobiles, corrections in Rel-5 and onwards were judged to be sufficient.

The misalignment among 3GPP specifications leads to undesirable effects and call drops in the CS domain, because ciphering and/or integrity protection fails. In that end, CN1 informed all affected Working Groups via LS in N1-040501 to verify CN1's understanding and if so, align their respective specifications accordingly.

CN1 has approved Rel-5/6 CRs in NP-040099 and N1-040498 in CN1#33, and further in N1-041074, N1-041075 in CN1#34.

SA3 informed CN1 in N1-041319 (S3-040436) that SA3 shared the understanding of CN1 in regards to the inconsistency on key set use after intersystem handover if AKA was run prior to intersystem handover, and aligned TS 33.102 accordingly.

RAN3 informed CN1 in N1-041321 (R3-040944) that CN1's understanding was correct that the MSC can provide only one key set to the RNC with the RANAP Relocation Request message. The key set provided in the message will be used by RNC after the handover.

After exchange of a few more LSes between CN1 and RAN2 (N1-041322, N1-041519), RAN2 finally informed CN1#37 in N1-042013 (R2-042611) that RAN2 will not align their TS 25.331 with approved stage 2 and stage 3 in other Working Groups. In this LS RAN2 states:

"To introduce this change now would lead to many UEs which are using the current version of the specifications to suffer more problems whenever the proposed behaviour will occur. It is also noted that because the situation raised does not exist in current network deployments, the impact of not accepting this change will be minimal."

CN1#37's understanding and response to RAN2's conclusions are:

1. RAN2 does acknowledge that the problem exists, but yet is not willing to change their specification in Rel-5 and onwards.

2. In CN1's view, the statement about *"pre-Rel-5 UEs suffering more problems when the proposed behaviours occur"* is incorrect. Those UEs would continue behaving as today, i.e. drop the call if late AKA happens before the handover.

There is at least one MSC implementation that would perform late AKA. The reason for the situation not to exist in the current deployments at this time is that the function can be switched off by the operator to avoid 'late AKA', in order not to cause troubles with existing R99 mobiles after handover. But this is at the cost of reduced security in the system and as such, for Rel-5/6 this 'security hole' must be closed. As an example, in GSM it is possible that MSC omits authentication for a specific access, because subscriber was authenticated in a previous access. When MSC then starts ciphering and algorithms supported in MSC and MS does not match, BSC then may choose 'no encryption' for the connection (GSM TS 12.03, chapter 4.3.1). In this case, MSC should do a 'late authentication' after it realizes that the connection will be unencrypted (GSM TS 12.03, chapter 6.2.1).

If an operator chooses to enable the feature in Rel-5, the system would fail. The result would be increased call drops, decreased revenue for operators and a bad user perception.

At this junction, CN1 would like to bring the issue to the attention of the SA plenary and to seek guidance.

2. Actions:

To SA group.

ACTION: CN1 kindly requests SA to provide a way forward on this issue. Either RAN2 shall align their specification with SA3 and CN1 from Rel-5 onwards, or CRs must be produced to revert the already plenary approved CRs by SA3 and CN1, and accepting the flaw in the system that the inter-system handover from GERAN to UMTS procedures after re-authentication would always fail, if the handover occurred before the new keys were taken into use.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050271
Sydney, Australia, 14-18 February 2005

Title: Reply LS (to R3-041648) on MBMS Information Elements over Iu interface
Response to: LS (N1-042014/R3-041648) on "MBMS Information Elements over Iu interface"
Release: Rel-6
Work Item: MBMS
Source: CN1
To: RAN3
Cc: GERAN2, SA2, SA4, CN3, CN4, RAN2

Contact Person:
Name: Christian Herrero
Tel. Number: +46 46231812
E-mail Address: christian.Herrero@ericsson.com

Attachments: None

---

1. Overall Description:

CN1 would like to thank RAN3 for their LS in N1-042014/R3-041648.

CN1 was asked to answer several questions made by RAN3, namely:

MBMS PTP RAB ID

RAN3 plan to code this IE in RANAP protocol as follows:
This element uniquely identifies a MBMS PTP radio bearer for a particular UE. The value is used in the RNC to relate MBMS PTP Radio Bearers to a MBMS RAB. The content of this information element is transferred unchanged from the SGSN via the RNC to the UE by RANAP messages and RRC messages.
The element contains binary representation of the Network Service Access Point Identifier (NSAPI). This identifier is coded in the PTP RAB ID element as BIT STRING (8) in accordance with the coding of the NSAPI IE in TS 24.008.
► RAN3 would be glad to receive confirmation from RAN2 and CN1 about consistent coding and handling of this IE in TS 24.008 and TS 25.331.

CN1 would like to inform RAN3 that the RAB id has the same format as the NSAPI and it is 1 octet as already identified by RAN3. Furthermore, CN1 would like to point out that the coding of the RAB id and NSAPI (as currently defined by TS 25.331 and TS 24.008 respectively) is consistent.

IP Multicast Address and APN

These IEs should remain transparent in RAN. Thus they should be coded in RANAP as transparent container i.e. OCTET STRING.
► RAN3 would to ask CN1 and CN4 whether these IEs have fixed length and where their coding is described

CN1 would like to indicate that the IP Multicast address and the APN parameters are transparent to the RAN via the core network protocols specified by CN1. In addition, the IP Multicast address is coded as a Packet Data Protocol address IE, which is defined in TS 24.008, sub-clause 10.5.6.4. This IE has a variable length from 3 to 19 octets. The length of the IP Multicast address varies depending on whether IPv4 (with a length of 4 octets) or IPv6 (with a length of 16 octets) is used. Additionally, the APN is encoded as an Access Point Name (APN) IE (defined in the sub-clause 10.5.6.1 of TS 24.008) with a minimum length of 3 octets and a maximum length of 102 octets.

2. Actions:

To RAN3 group.

ACTION: CN1 kindly requests RAN3 to take note of the information provided above.

3. Date of Next TSG-CN1 Meetings:

CN1_37	14th – 18th February 2005	Sydney, Australia
CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050272
Sydney, Australia, 14-18 February 2005

Title: LS on 3rd party registration and shared public user identities
Response to: N1-042093 LS on 3rd party registration and shared public user identities from SA2

Release: Rel-6
Work Item: IMS2

Source: CN1
To: SA2
Cc:

Contact Person:
Name: **Peter Leis**
Tel. Number: +49 89 636 75208
E-mail Address: peter.leis@siemens.com

Attachments:

---

1. Overall Description:

CN WG1 thanks SA WG2 for their LS on 3rd party registration and shared public user identities (S2-043858 / N1-042093).

A solution based on additional information in the contact header as proposed in the LS from SA2 is not feasible as this would lead the application server to fork requests .In addition this breaks the current concept that from an AS point of view there the AS is the only contact and that the AS does only have one binding (S-CSCF/public user ID).

Another solution was proposed to solve the issue. This proposal is based on a modified 3rd party REGISTER, i.e. the S-CSCF sets the timer in expires parameter of the 3rd party REGISTER sent to the AS to the longest value of expiration that is available for that particular public User ID. This solution has no backward compatibility issues from the AS point of view. Using this solution the AS will not have knowledge of individual contacts (terminals) for the public user ID. However, further study of the impacts of filter criteria handling on this solution is needed. The solution was not agreed.

In case the AS wants to get detailed information of the status of the public user ID then subscription to the reg-event package is the appropriate mechanism.

2. Actions:

To SA2 group.

ACTION:
CN1 would like to get guidance whether a solution based on expires parameter as proposed is acceptable from an architectural point of view.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050273
Sydney, Australia, 14-18 February 2005

Title: Reply LS on "S-CSCF client address comparisons and their affect on de-registrations"
Response to: LS (N1-050006) on "S-CSCF client address comparisons and their affect on de-registrations" from CN4
Release: Rel-6
Work Item: IMS2

Source: CN1
To: CN4
Cc:

Contact Person:
Name: Varga József
Tel. Number: +36209849040
E-mail Address: jozsef.varga@nokia.com

Attachments: None.

---

1. Overall Description:

CN1 thanks CN4 for their LS on CSCF client address comparisons and their affect on de-registrations.

It is CN1's understanding that the client address of the S-CSCF (SIP-URI) can change any time. According to a note in TS 24.229 (Rel-6 v.6.5.1, see chapter 5.4.1.2.1) "S-CSCF may include in its SIP URI the transport protocol and the port number where it wants to be contacted", thus this implies that the SIP URI of the S-CSCF may change at any time.

2. Actions:

To CN4 group.

ACTION: CN1 kindly asks CN4 to note the above answer from CN1.

3. Date of Next TSG-CN1 Meetings:

CN1_37	14th – 18th February 2005	Sidney, Australia
CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050276
Sydney, Australia, 14-18 February 2005

Title: LS on PS handover and Robust Header Compression (RoHC) Context Relocation
Response to: Reply LS (R2-050299/N1-050035) on the PS Handover work from RAN2
Release: Rel-6
Work Item: Support of Conversational Services in A/Gb Mode via the PS Domain

Source: CN1
To: RAN2
Cc: GERAN2, SA2, RAN3, CN4

Contact Person:
Name: Robert Zaus
E-mail Address: robert.zaus@siemens.com

Attachments: none

---

1. Overall Description:

CN1 would like to thank RAN2 for the liaison statement on PS Handover work (R2-050299/N1-050035).

With regard to the assumptions made by RAN2, CN1 confirm that:

1. There is no requirement for a lossless inter-RAT PS handover from CN1's side.

2. CN1 also assume that the header compression contexts for Robust Header Compression (RoHC) will not be transferred to the target system during PS handover and will need to be re-established after completion of the PS handover.

2. Actions:

none.

3. Date of Next TSG-CN1 Meetings:

CN1_37	14th – 18th February 2005	Sydney, Australia
CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050277
Sydney, Australia, 14-18 February 2005

Title: Reply LS on IP multimedia messaging capabilities
Response to: Reply LS (S1-050159) on IP multimedia group management and messaging capabilities
Release: Rel-6
Work Item: IMS2

Source: CN1
To: SA1
Cc: CN

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

Attachments: none

---

1. Overall Description:

CN1 thanks SA1 for the reply, giving clarifications and guidelines on IP multimedia group management and messaging capabilities.

- CN1 note that SA1 does not want to do changes to their TS structure.
- CN1 can inform SA1 that a CR to 24.247 has been agreed in CN1 #37 regarding the ability to give indication to the peer entity when typing is in progress ('Is typing' or 'isComposing'), thus this requirement should now be fulfilled by stage 3.
- CN1 can inform SA1 that CRs to 24.247 have been agreed in CN1 #37 regarding the ability to distribute the messages to several recipients based on the delivery list, thus this requirement should now be fulfilled by stage 3. The CRs introduce the two mechanisms as outlined by stage 2.

2. Actions:

none.

3. Date of Next TSG-CN1 Meetings:

CT1 #38	15th – 19th of April 2005	Cancun, Mexico
CT1 #39	25th – 29th of August 2005	London

3GPP TSG-CN1 Meeting #37 Tdoc N1-050278
Sydney, Australia, 14-18 February 2005

Title: LS on provisioning of the UE RAC and START_PS to the network

Response to: LS (GP-050575/ N1-050097) on method for provisioning of the UE RAC and START_PS to the network.

Release: Rel-6

Work Item: Support of Conversational Services in A/Gb Mode via the PS Domain

Source: CN1

To: GERAN2, RAN2, RAN3

Cc: ---

Contact Person:
Name: Robert Zaus
E-mail Address: robert.zaus@siemens.com

Attachments: N1-050404 [CR 24.008 – 950 rev2; agreed by CN1].

---

1. Overall Description:

CN1 would like to thank GERAN 2 for the liaison statement on Method for provisioning of the UE RAC and START_PS to the network (GP-050575/ N1-050097).

CN1 have considered the methods proposed by GERAN 2 for providing the parameters UE RAC and START PS to the network and have agreed the attached CR to TS 24.008. The agreed method deviates from the example CR sent by GERAN 2 in a few points:

i) The information is sent by the mobile station during the GPRS attach or routing area update procedure, when the SGSN explicitly requests the mobile station in the Attach Accept or Routing Area Update Accept message to do so. Accordingly, the information will be included by the MS in the **Attach Complete** or **Routing Area Update Complete** message. – This allows some optimizations at the radio interface, e.g. the SGSN need not request the information during each intra-SGSN routing area update.

ii) The parameters UE RAC and START_PS will be transmitted in a new information element "Inter RAT information container". This is an information element of variable length, with a minimum length of 3 and a **maximum length of 40 octets**. – CN1 considered it appropriate to define a fixed maximum length, since the information needs to be stored by the SGSN potentially for each subscriber registered with the SGSN.

When setting an upper limit of 40 octets, corresponding to a value part of 38 octets, CN1 made the assumption that the MS would include only one of the two parameters "Predefined configuration status information" and "Predefined configuration status information compressed", and only one of the two parameters "UE radio access capability" and "UE radio access capability compressed" in the INTER RAT HANDOVER INFO (see TS 25.331, subclause 10.2.16d). Since the compressed encoding was introduced in Rel-5 and PS Inter-RAT Handover is a Rel-6 feature, CN1 further assumed that all RNCs supporting PS Inter-RAT Handover would be able to decode the compressed format of the parameters.

1. CN1 kindly ask **RAN2** to check whether these assumptions are correct and whether 38 octets are sufficient to store the necessary UE RAC and START_PS information.

2. CN1 also ask **RAN2** to indicate whether it is correct that the INTER RAT HANDOVER INFO from TS 25.331, subclause 10.2.16d) is the information to be included in the "Inter RAT information container" in TS 24.008.

Concerning the transport of the UE RAC and START_PS information to the target RNC during a GERAN to UTRAN inter-RAT PS handover, CN1 would like to make the following proposal to **GERAN 2** and **RAN3**:

- Since the SGSN needs to store this information anyway, and
- the serving BSC will forget the information each time the packet flow context is released, and
- the information is sent to the BSC only for the purpose to be sent back via the SGSN to the target RNC,

CN1 would like to propose that the information is treated by the SGSN in the following way:
The information is stored in the SGSN and never sent to the serving BSC. At inter-system handover from GERAN to UTRAN, the SGSN includes the information as RANAP parameter in the RANAP Relocation Request message to the target RNC.

This would allow to avoid unnecessary transmissions and re-transmissions of the UE RAC and START_PS information via the Gb interface.

Please note that the same handling is already used for the transport of the UMTS Ciphering Key and Integrity Key to the target RNC during circuit-switched inter-system handover from GERAN to UTRAN.

If CN1's proposal is adopted, GERAN 2 would probably need to specify a mechanism how the serving BSC can determine whether the SGSN supports PS inter-system handover from GERAN to UTRAN (e.g. by local administration in the BSC or by BSSGP signalling between BSC and SGSN).

2. Actions:

To GERAN 2, RAN2, RAN3 group.

ACTION:

CN1 asks **GERAN2**:
to note the attached CR.

CN1 asks **RAN2**:
to answer CN1's questions and to confirm that the size of the "Inter RAT information container" is sufficient.

CN1 asks **GERAN2 and RAN3**:
to take CN1's proposal for the transport of the UE RAC and START_PS information from the SGSN to the target RNC into account.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050279
Sydney, Australia, 14-18 February 2004

Title: Reply LS on "Misalignment between VGCS stage 1 and 2"
Response to: LS (N1-050252) on "Misalignment between VGCS stage 1 and 2" from SA1
Release: Rel-7
Work Item: EVGCS

Source: CN1
To: SA1
Cc:

Contact Person:
Name: Sonia Garapaty
Tel. Number: +1 972 685 5110
E-mail Address: sonia.garapaty@nortel.com

Attachments: None.

---

1. Overall Description:

CN1 thanks SA1 for their LS on misalignment between the VGCS Stage 1 and Stage 2.

It is CN1's understanding that the VGCS Stage 1 requirement, where the first subscriber becomes the talker if more than one subscriber indicates an emergency situation, included in TS 42.068 Section 4 o) is a Rel-7 requirement. CN1 plans to make the necessary changes in Rel-7 to Stage 2 TS 43.068 to satisfy the new Stage 1 requirement.

2. Actions:

To SA1 group.

ACTION: CN1 kindly asks SA1 to note the above answer from CN1.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37
Sydney, Australia, 14-18 February 2005

Tdoc N1-050354
Revision of N1-050327

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.234** **CR** **20** ⌘ **rev** **2** ⌘ Current version: **6.1.1** ⌘

*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:	⌘	Fallback to full authentication
Source:	⌘	Ericsson, Nokia
Work item code:	⌘	WLAN
Date:	⌘	15/02/2005
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:	⌘	At SA3#36 the agreed CR in S3-041110 introduced a new requirement into TS 33.234, which is now implemented in the latest version of the specification (i.e. v6.3.0). The requirement mandates the 3GPP AAA server to send a pseudonym every time a re-authentication identity is sent to the WLAN UE. Therefore, fallback to full authentication is always possible.
Summary of change:	⌘	The stage 2 requirement is introduced into TS 24.234.
Consequences if not approved:	⌘	Misalignment with stage 2 (i.e. TS 33.234) remains. Therefore, mandatory requirements will not be included in the appropriate stage 3 specification (i.e. TS 24.234). This may lead to different 3GPP AAA server implementations.

Clauses affected:	⌘	

		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.

6.1.1.3.5 Re-authentication

The 3GPP AAA server shall support re-authentication as specified in the 3GPP TS 33.234 [5].

Re-authentication should be enabled in the 3GPP AAA server. If re-authentication is enabled, the re-authentication may be full or fast, as follows:

- Full re-authentication means that a new full authentication procedure shall take place as the initial authentication procedure, where all keys are generated afresh in both the (U)SIM and network. Full re-authentication requires that the WLAN UE sends pseudonym or permanent IMSI-based identity.

- Fast re-authentication means that a new authentication procedure takes place in which Master Key and Transient EAP Keys are not generated in both the (U)SIM and network, but reused from the previous authentication process to generate the remaining keys necessary for this procedure. Fast re-authentication requires that the WLAN UE sends re-authentication identity.

The decision of using fast re-authentication is taken in the 3GPP AAA server depending on operator's policies. Operator's policies regarding fast re-authentication may contain for example, a timer to control start of fast re-authentication, a counter to control the maximum number of allowed fast re-authentications before a full EAP authentication shall be initiated towards the WLAN UE or a restriction on whether fast re-authentication is allowed to visiting subscribers.

The 3GPP AAA server indicates to the WLAN UE the decision of using fast re-authentication by means of sending the re-authentication identity in the EAP authentication procedure (i.e. in EAP-Request/AKA/-Challenge or EAP-Request/AKA/-re-authentication or EAP-Request/SIM/Challenge or EAP-Request/SIM/re-authentication messages). On each fast re-authentication procedure the 3GPP AAA server has the ultimate point of decision of whether to continue with the ongoing fast re-authentication procedure or to defer to a full re-authentication. Therefore, whenever the 3GPP AAA server sends a re-authentication identity to the WLAN UE, the 3GPP AAA server shall also include a pseudonym when allowed by the draft-haverinen-pppext-eap-sim [10] and draft-arkko-pppext-eap-aka [9]. In this way, the WLAN UE retains a pseudonym if the 3GPP AAA server defers to full authentication.

NOTE 1: In the current version of the draft-haverinen-pppext-eap-sim [10] and draft-arkko-pppext-eap-aka [9] the pseudonym (i.e. AT_NEXT_PSEUDONYM attribute) can only be sent during a full re-authentication procedure (i.e. in EAP-Request/SIM/Challenge or EAP-Request/AKA/Challenge).

NOTE 2: The use of fast re-authentication implies to save power consumption in the WLAN UE and processing time in both the WLAN UE and the 3GPP AAA server. However, when the fast re-authentication is used through a low trusted I-WLAN, it is strongly recommended to refresh the keys using full re-authentication. The use of fast re-authentication should be left for situations in which the user is accessing a high trusted I-WLAN.

The full and fast re-authentication signalling flows are described in 3GPP TS 33.234 [5].

3GPP TSG-CN1 Meeting #37 Tdoc N1-050371
Sydney, Australia, 14-18 February 2005

Title: **Reply LS on Application Charging ID**

Response to: **LS (N1-050023/S5-044780) on "**LS on Application Charging ID for PoC**"**

Release: **Rel-6**

Work Item: **Support for PoC**

Source: **CN1**

To: **SA5**

CC: **SA2**

Contact Person:
Name: Chang Duan
Tel. Number: +86 (10) 82882604
E-mail Address: chang.duan@huawei.com

---

1. Overall Description:

CN1 would like to thank SA5 for their LS on the Application Charging ID for PoC.

CN1 has discussed the issue of Application Charging ID (ACID) and felt that further information on the ACID would be helpful in guiding CN1's future work on it. Therefore CN1 kindly asks SA5 to give further clarification on questions regarding the usage and functionality of this ACID as listed in the action part, in which CN1 is particularly interested.

CN1 expects that when the information requested is available, documentation will take at least two meeting cycles, and possible more if IETF changes are required to RFC 3455 to accommodate these requirements. Such work is therefore likely to extend beyond release 6.

2. Actions:

To SA5 group.

ACTION: Provide information and clarification on the following:

- Which entities are required to generate or understand ACID;
- Whether it is used for a single application or multiple applications;
- Which entities should include this ACID in its CDRs;
- The lifetime of this ACID;
- How ACID is transmitted, in particular, whether ACID is transmitted in a SIP request and response.

3. Date of Next CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050376
Sydney, Australia, 14-18 February 2005

Title: **Alignment of specifications between CN1 and SA3 with respect to fallback to full authentication**

Response to:

Release: Rel-6

Work Item: WLAN-IW

Source: CN1

To: SA3

Cc:

Contact Person:
Name: Paul Sitch
E-mail Address: paul.sitch@nokia.com

Attachments: N1-050354

---

1. Overall Description:

CN1 would like to draw SA3 attention to the following issue:

SA3 recently introduced the requirement that the 3GPP AAA server shall always send a pseudonym every time a re-authentication identity is sent to the WLAN UE, in order that fallback to full authentication is always possible. On attempting to align the CN1 specification with this new requirement, it was noted that the EAP-SIM and EAP-AKA specifications, to which our specifications shall comply, state that a pseudonym can be sent only during full authentication, and not during re-authentication. CN1 therefore agreed the text as indicated in the attached CR.

2. Actions:

CN1 kindly ask SA3 to consider the attached CR that was agreed in CN1#37 and align the SA3 specification, if appropriate.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN WG1 Meeting #37 **N1-050383**
Sydney, AUSTRALIA. 14th to 18th February 2005.

Source:	**CN1**
Title:	**Reply LS on transport of HSS address**
Agenda item:	**3**
To:	**SA2**
CC:	**CN4**

Contact Person:

Name: Alf Heidermark

Tel nr: +46 87273894

E-mail Address: Alf Heidermark@ericsson.com

---

1. Overall Description:

CN1 thank SA2 on their LS on transport of HSS address.

The described functionality could be achieved by means of an optional P-Header included by the I-CSCF when forwarding the SIP REGISTER or INVITE request. The I-CSCF would insert the HSS address that it received in the corresponding query to the SLF in that header. The S-CSCF would use this HSS address for the destination of the corresponding Cx requests and omit the query to the SLF.
This P-Header would have to be defined in an IETF RFC as an extension of the SIP protocol. A draft including a solution (draft-camarillo-sipping-user-database-00.txt) has been submitted in order to be discussed at the next IETF meeting 6th -11th of March.

2. Actions:

To SA2.

ACTION: CN1 kindly ask SA2 to take the proposed answer into consideration.

3. Date of Next SA2 Meetings:

CT1#38	25th - 29th April 2005	Cancun, Mexico
CT1#39	29th Aug - 2nd Sept 2005	London, Great Britain

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.008** **CR** **930** ⌘ **rev** **4** ⌘ Current version: **6.7.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Transparent data call request in dual mode case
Source:	⌘	Nokia
Work item code:	⌘	TEI-6
Date:	⌘	02/02/2005
Category:	⌘	**C**
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:	⌘	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 know that an 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:	⌘	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 a GSM radio network

Clauses affected:	⌘	10.5.4.5			
Other specs affected:	⌘	**Y** / **N**		⌘	
		X /	Other core specifications		27.001, 48.008
		/ **X**	Test specifications		
		/ **X**	O&M Specifications		

Other comments:	⌘	It is proposed to consider this CR as release independent and implementable on earlier releases also.

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.

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 ext	radio channel requirement		co-ding std	trans fer mode	information transfer capability			octet 3
0/1 ext	0 co-ding	CTM 0 spare		speech version indication				octet 3a *
0/1 ext	0 co-ding	0 spare	0 Spare	Speech version Indication				octet 3b etc*
1 ext	comp -ress.	Structure		dupl. mode	confi gur.	NIRR	esta-bli.	octet 4*
0/1 ext	0 access id.	0	rate adaption		signalling access protocol			octet 5*
0/1 ext	Other ITC		Other rate adaption		0 Spare	0	0	octet 5a*
1 ext	Hdr/ noHdr	Multi frame	Mode	LLI	Assig nor/e	Inb. neg	0 Spare	octet 5b*
0/1 ext	0 layer 1 id.	1	User information layer 1 protocol				sync/ async	octet 6*
0/1 ext	numb. stop bits	nego-tia-tion	numb. data bits	user rate				octet 6a*
0/1 ext	intermed. rate		NIC on TX	NIC on RX	Parity			octet 6b*
0/1 ext	connection element		modem type					octet 6c*
0/1 ext	Other modem type		Fixed network user rate					octet 6d*
0/1 ext	Acceptable channel codings				Maximum number of traffic channels			octet 6e*
0/1 ext	UIMI		Wanted air interface user rate					octet 6f*
1 ext	Acceptable channel codings Extended			Asymmetry Indication	0 Spare	0		octet 6g*
1 ext	1 layer 2 id.	0	User information 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-CN1 Meeting #37 **Tdoc N1-050403**
Sydney, Australia, 14-18 February 2004

Source: Vodafone

Title: DISC Proposed Changes to TR 33.878

Agenda item: 7.1

Document for: APPROVAL

A number of comments have been made on TR 33.878 "Security Aspects of Early IMS" in N1-050218. This document proposes changes to TR 33.878 to address these comments.

*** Proposed Changes to TR 33.878 v1.0.0 ***

Introduction

3GPP IMS provides an IP-based session control capability based on the SIP protocol. IMS can be used to enable services such as push-to-talk, instant messaging, presence and conferencing. It is understood that "early" implementations of these services will exist that are not fully compliant with 3GPP IMS. For example, it has been recognized that although 3GPP IMS uses exclusively IPv6, as specified in clause 5.1 of TS 23.221 [13], there will exist IMS implementations based on IPv4 (TR 23.981 [1]).

Non-compliance with IPv6 is not the only difference between early IMS implementations and fully 3GPP compliant implementations. In particular, it is expected that there will be a need to deploy some IMS-based services before products are available which fully support the 3GPP IMS security features defined in TS 33.203 [2]. Non-compliance with TS 33.203 security features is expected to be a problem mainly at the UE side, because of the potential lack of support of the USIM/ISIM interface (especially in 2G-only devices) and because of the potential inability to support IPsec on some UE platforms.

It is acknowledged that early IMS implementations will exist which do not support all the security features specified in TS 33.203~~Although full support of 3GPP TS 33.203 security features is preferred from a security perspective, it is acknowledged that early IMS implementations will exist which do not support these features~~. Therefore, there is a need to ensure that simple, yet adequately secure, mechanisms are in place to protect against the most significant security threats that will exist in early IMS implementations. ~~Furthermore, to maximise interoperability, it is important that these mechanisms are adequately standardised.~~

1 Scope

The present document ~~specifies~~ documents an interim security solution for early IMS implementations that are not fully compliant with the IMS security architecture specified in TS 33.203 [2].

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 23.981: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Interworking aspects and migration scenarios for IPv4 based IMS Implementations".

[2] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".

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

[4] 3GPP TS 29.061: "3rd Generation Partnership Project; Technical Specification Group Core Network; Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[5] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[6] IETF RFC 3261: "Session Initiation Protocol".

[7] 3GPP TS 24.229: "3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[8] 3GPP TS 23.003: "3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification".

[9] 3GPP TS 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[10] 3GPP TS 29.228: "3rd Generation Partnership Project; Technical Specification Group Core Network; IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents".

[11] draft-ietf-aaa-diameter-nasreq-17.txt (July 2004), "Diameter Network Access Server Application", work in progress.

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

[12] 3GPP TS 29.229: "3rd Generation Partnership Project; Technical Specification Group Core Network; Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[13] 3GPP TS 23.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architectural requirements".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 21.905 [9] and the following apply.

Early IMS: a UE or network element implementing the early IMS security solution specified in the present document.

Fully compliant IMS: a UE or network element implementing the IMS security solution specified in TS 33.203 [2].

3.2 Symbols

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

Cx Reference Point between a CSCF and an HSS.
Gi Reference point between GPRS and an external packet data network

3.3 Abbreviations

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

AAA Authentication Authorisation Accounting
ABNF Augmented Backus-Naur Form
APN Access Point Name
AVP Attribute-Value Pair
CSCF Call/Session Control Function
GGSN Gateway GPRS Support Node
HSS Home Subscriber Server
I-CSCF Interrogating CSCF
ICID IM CN subsystem Charging Identifier
IM IP Multimedia
IMPI IM Private Identity
IMPU IM Public Identity
IMS IP Multimedia Subsystem
IP Internet Protocol
IPSec IP Security protocol
ISIM IMS Subscriber Identity Module
NAT Network Address Translation
P-CSCF Proxy-CSCF
PDP Packet Data Protocol
RFC Request For Comments
S-CSCF Serving-CSCF
SGSN Serving GPRS Support Node
SIP Session Initiation Protocol
SLF Server Locator Function
UE User Equipment
URI Uniform Resource Identifier

4 Requirements

Low impact on existing entities: Any early IMS security mechanisms should be such that impacts on existing entities, especially on the UE, are minimised and would be quick to implement. It is especially important to minimise impact on the UE to maximise interoperability with early IMS UEs. The mechanisms should be quick to implement so that the window of opportunity for the early IMS security solution is not missed.

Adequate level of security: Although it is recognised that the early IMS security solution will be simpler than the fully compliant IMS security solution, it should still provide an adequate level of security to protect against the most significant security threats that will exist in early IMS implementations. As a guide, the strength of subscriber authentication should be comparable to the level of authentication provided for existing chargeable services in mobile networks.

Smooth and cost effective migration path to fully compliant solution: Clearly, any security mechanisms developed for early IMS systems will provide a lower level of protection compared with that offered by the fully compliant IMS security solution. The security mechanisms developed for early IMS systems should therefore be considered as an interim solution and migration to the fully compliant IMS security solution should take place as soon as suitable products become available at an acceptable cost. In particular, the early IMS security solution should not be used as a long-term replacement for the fully compliant IMS security solution. It is important that the early IMS security solution allows a smooth and cost-effective migration path to the fully compliant IMS security solution.

Co-existence with fully compliant solution: It is clear that UEs supporting the early IMS security solution will need to be supported even after fully compliant IMS UEs are deployed. The early IMS security solution should therefore be able to co-exist with the fully compliant IMS security solution. In particular, it shall be possible for the SIP/IP core to differentiate between a subscription using early IMS security mechanisms and a subscription using the fully compliant IMS security solution.

Protection against bidding down: It should not be possible for an attacker to force the use of the early IMS security solution when both the UE and the network support the fully compliant IMS security solution.

No restrictions on the type of charging model: Compared with fully compliant IMS security solution, the early IMS security solution should not impose any restrictions on the type of charging model that can be adopted.

A single early IMS security solution: Interfaces that are impacted by the early IMS security solution should be adequately documented to ensure interoperability between vendors. ~~**Standardisation of a single early IMS security solution:** Interfaces that are impacted by the early IMS security solution should be adequately standardised to ensure interoperability between vendors. To avoid unnecessary complexity, a single early IMS security solution should be standardised.~~

Support access over 3GPP PS domain: It is a requirement is to support secure access over the 3GPP PS domain (including GSM/GPRS and UMTS access).

Low impact on provisioning: The impact on provisioning should be low compared with the fully compliant IMS security solution.

5 Threat scenarios

To understand what controls are needed to address the security requirements, it is useful to describe some of the threat scenarios.

NOTE: There are many other threats, which are outside the scope of this TR.

5.1 Impersonation on IMS level using the identity of an innocent user

The scenario proceeds as follows:

- Attacker A attaches to GPRS, GGSN allocates IP address, IP_A
- Attacker A registers in the IMS using his IMS identity, ID_A
- Attacker A sends SIP invite using his own source IP address (IP_A) but with the IMS identity of B (ID_B).

If the binding between the IP address on the bearer level, and the public and private user identities is not checked then the attacker will succeed, i.e. A pays for IP connectivity but IMS service is fraudulently charged to B. The fraud situation is made worse if IP flow based charging is used to 'zero rate' the IP connectivity.

The major problem is however that without this binding multiple users within a group "of friends" could sequentially (or possibly simultaneously) share B's private/public user identities, and thus all get (say) the push-to-talk service by just one of the group paying a monthly subscription. Without protection against this attack, operators could be restricted to IP connectivity based tariffs and, in particular, would be unable to offer bundled tariffs. This is unlikely to provide sufficiently flexibility in today's market place.

5.2 IP spoofing

The scenario proceeds as follows:

- User B attaches to GPRS, GGSN allocates IP address, IP_B
- User B registers in the IMS using his IMS identity, ID_B
- Attacker A sends SIP messages using his own IMS identity (ID_A) but with the source IP address of B (IP_B)

If the binding between the IP address that the GGSN allocated the UE in the PDP context activation and the source IP address in subsequent packets is not checked then the attacker will succeed, i.e. A pays for IMS service but IP connectivity is fraudulently charged to B. Note that this attack only makes sense for IMS services with outgoing traffic only because the attacker will not receive any incoming packets addressed to the IMS identity that he is impersonating.

5.3 Combined threat scenario

The scenario proceeds as follows:

- User B attaches to GPRS, GGSN allocates IP address, IP_B
- User B registers in the IMS using his IMS identity, ID_B
- Attacker A sends SIP messages using IMS identity (ID_B) and source IP address (IP_B)

If the bindings mentioned in the scenarios in clause 5.1 and 5.2 are not checked then the attacker will succeed, i.e. A fraudulently charges both IP connectivity and the IMS service to B. Note this attack only makes sense for IMS services with outgoing traffic only because the attacker will not receive any incoming packets addressed to the IMS identity that he is impersonating.

6 Specification

6.1 Overview

6.1.1 Security Mechanism

The early IMS security solution works by creating a secure binding in the HSS between the public/private user identity (SIP-level identity) and the IP address currently allocated to the user at the GPRS level (bearer/network level identity). Therefore, IMS level signaling, and especially the IMS identities claimed by a user, can be connected securely to the PS domain bearer level security context.

The GGSN, terminates each user's PDP context and has assurance that the IMSI used within this PDP context is authenticated. The GGSN shall provide the user's IP address, IMSI and MSISDN to a RADIUS server in the HSS over the Gi interface when a PDP context is activated towards the IMS system. The HSS has a binding between the IMSI and/or MSISDN and the IMPI and IMPU(s), and is therefore able to store the currently assigned IP address from the GGSN against the user's IMPI and/or IMPU(s). The precise way of the handling of these identities in the HSS is outside the scope of standardization. The GGSN informs the HSS when the PDP context is deactivated/modified so that the stored IP address can be updated in the HSS. When the S-CSCF receives a SIP registration request or any subsequent requests for a given IMPU, it checks that the IP address in the SIP header (verified by the network) matches the IP address that was stored against that subscriber's IMPU in the HSS.

The mechanism assumes that the GGSN does not allow a UE to successfully transmit an IP packet with a source IP address that is different to the one assigned during PDP context activation. In other words, the GGSN must prevent "source IP spoofing". The mechanism also assumes that the P-CSCF checks that the source IP address in the SIP header is the same as the source IP address in the IP header received from the UE (the assumption here, as well as for the full security solution, is that no NAT is present between the GGSN and the P-CSCF).

The mechanism prevents an attacker from using his own IP address in the IP header but spoofing someone else's IMS identity or IP address in the SIP header, so that he pays for GPRS level charges, but not for IMS level charges. The mechanism also prevents an attacker spoofing the address in the IP header so that he does not pay for GPRS charges. It therefore counters the threat scenarios given in clause 5 above.

6.1.2 Restrictions Imposed by Early IMS Security

The mechanism assumes that only one contact IP address is associated with one IMPI. Furthermore, the mechanism supports the case that there may be several IMPUs associated with one IMPI, but one IMPU is associated with only one IMPI.

In early IMS security, the IMS user authentication is performed by linking the IMS registration (based on an IMPI) to a PDP context (based on an authenticated IMSI). The mechanism here assumes that there is a one-to-one relationship between the IMSI for bearer access and the IMPI for IMS access.

For the purposes of this present document, an APN, which is used for IMS services, is called an IMS APN. An IMS APN may be also used for non-IMS services. The mechanism described in this present document further adds a restriction that there is only one APN for accessing IMS for a PLMN and that all active PDP contexts, for a single UE, associated with that IMS APN use the same IP address at any given time.

The Early IMS security mechanism relies on the Via header remaining unchanged between the UE and the S-CSCF, therefore topology hiding cannot be used.

Early IMS security requires the GGSN to be in the home network.

The interim solution works with UEs that contain a SIM or a USIM, whereas full IMS security requires a USIM or ISIM.

The interim solution does not authenticate at the IMS level. Instead, it relies on bearer level security at the GPRS or UMTS PS level. Because there is no key agreement, IPsec security associations are not set up between UE and P-CSCF, as they are in the full IMS security solution.

The solution works by binding the IMS level transactions to the GPRS or UMTS PS domain security association established at a GPRS or UMTS PS domain level. In doing so, it creates a dependency between SIP and the PS bearer, which does not exist with the full IMS security solution. This means that the interim solution does not provide as high a

degree of access network independency as the full solution. In particular, the solution does not currently support scenarios where IMS services are offered over WLAN. If support for WLAN access is required then the full solution must be used or the interim solution must be extended to cover WLAN access.
Early IMS security derives the public user identity used in the REGISTER request from the IMSI. Consequently, the same public user identity cannot be simultaneously registered from multiple terminals, using only early IMS security registration procedures. However, registration of a public user identity from one terminal using early IMS security, and from another terminal using fully compliant IMS security is not precluded.

NOTE: The early IMS mechanism for security is completely independent of early IMS implementations based on IPv4. For example, an IPv4 based implementation may use the full IMS security solution in TS 33.203[2].

6.1.3 Early IMS Security and Logical Entities

In the following we use the terms P-CSCF and S-CSCF in a general sense to refer to components of an early IMS system. We note however that early IMS solutions may not have the same functionality split between SIP entities as defined in TS 23.228 [3]. Therefore, the requirements imposed on the SIP/IP core are specified in such a way that they are independent of the functionality split between SIP entities as far as possible. While the exact functionality split of the SIP/IP core may be left open, it is important that any changes to the Cx interface towards the HSS and changes to the interface towards the UE are standardised for vendor interoperability reasons.

6.2 Detailed specification

6.2.1 GGSN-HSS interaction

When receiving an Activate PDP Context Request message, based on operator policy, a GGSN supporting early IMS security shall send a RADIUS "Accounting-Request START" message to a AAA server attached to the HSS. The message shall include the mandatory fields defined in clause 16.4.3 of TS 29.061 [4] and the UE's IP address, MSISDN and IMSI. On receipt of the message, the HSS shall use the IMSI and/or the MSISDN to find the subscriber's IMPI (derived from IMSI) and then store the IP address against a suitable identity, e.g. the IMPI.

NOTE 1: It is assumed here that the RADIUS server attached to the HSS is different to the RADIUS server that the GGSN may use for access control and IP address assignment. However, according to TS 23.060 [5] there is no limitation on whether RADIUS servers for Accounting and Access control have to be separate or combined.

NOTE 2: It is also possible to utilize RADIUS to DIAMETER conversion in the interface between GGSN and HSS. This makes it possible to utilize the existing support for DIAMETER in the HSS. One possibility to implement the conversion is to re-use the AAA architecture of I-WLAN i.e. the 3GPP AAA Proxy or Server and its capability to perform RADIUS to DIAMETER conversion. It should be noted that the GGSN shall always uses RADIUS for this communication. Furthermore, it should be noted that DIAMETER is not mandatory to support in the HSS for communication with the GGSN.

GGSN shall not accept the activation of the PDP context if the accounting start request is not successfully handled by the HSS (e.g. a positive Create PDP Context Response should not be sent by the GGSN until the "Accounting-Request START" message is received or a negative Create PDP Context Response is sent after some RADIUS response timeout occurs). In particular, it shall not be possible to have an active PDP context associated with the IMS APN if the corresponding IP address is not stored in the HSS.
When the UE establishes its first PDP context for an IMS APN a new IP address is obtained, and the GGSN shall send an "Accounting-Request START" to the HSS with the assigned IP address. If this IP address is different from the IP address already stored in the HSS (i.e. the "old" IP address), the HSS shall start the 3GPP IMS HSS-initiated de-registration procedure, if the UE is IMS registered, using a Cx-RTR/Cx-RTA exchange, and delete the old IP address. The HSS stores the new IP address and confirms the "Accounting-Request START" to the GGSN when either the de-registration procedure is successfully completed or after a suitable time-out. The UE starts the IMS initial registration procedure. The HSS shall abandon the de-registration procedure when a new successful authentication for this user is signalled by the S-CSCF in a Cx-SAR message.
When all the PDP contexts are de-activated at the IMS APN of the GGSN, the GGSN sends an "Accounting-Request STOP" request to the HSS. The HSS checks the IP address indicated by the "Accounting-Request STOP" message against the IP address stored in the HSS. If they are the same, an HSS-initiated de-registration procedure shall be started, if the UE is registered, using a Cx-RTR/Cx-RTA exchange. In the case they are different, the HSS shall ignore the message.

6.2.2 Protection against IP address spoofing in GGSN

All GGSNs that offer connection to IMS shall implement measures to prevent source IP address spoofing. Specifically, a UE attached to the GGSN shall not be able to successfully transmit an IP packet with a source IP address that is different to the one assigned by the GGSN during PDP context activation. If IP address spoofing is detected the GGSN shall drop the packet. It shall be possible for the GGSN to log the event in its security log against the subscriber information (IMSI/MSISDN), e.g. based on operator configuration.

6.2.3 Impact on IMS registration and authentication procedures

A UE shall not be able to spoof its assigned IP address and successfully receive service from the IMS. The mechanisms in the following clauses shall be supported to prevent IP address spoofing in the IMS domain. The changes to the IMS registration and authentication procedures are detailed in the following clauses.

6.2.3.1 Procedures at the UE

On sending a REGISTER request in order to indicate support for early IMS security procedures, the UE shall not include an Authorization header field and not include a Security-Client header field. The From header, To header, Contact header, Expires header, Request URI, Supported header and a P-Asserted-Id header shall be set according clause 5.1.1.2 of TS 24.229 [7].

On receiving the 200 (OK) response to the REGISTER request, the UE shall handle the expiration time, the P-Associated-URI header field, and the Service-Route header field according clause 5.1.1.2 of TS 24.229 [7].

The UE shall support SIP compression as described in TS 24.229[7] subclause 8.1.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the UE creates the compartment is implementation specific.

NOTE 1: Early IMS security does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

NOTE 2: The UE shall not use the temporary public user identity used for registration in any subsequent SIP requests.

6.2.3.2 Procedures at the P-CSCF

NOTE: As specified in RFC 3261 [6], when the P-CSCF receives a SIP request from an early IMS UE, the P-CSCF checks the IP address in the "sent-by" parameter of the Via header field provided by the UE. If the "sent-by" parameter contains a domain name, or if it contains an IP address that differs from the packet source IP address, the P-CSCF adds a "received" parameter to that Via header field value. This parameter contains the source IP address from which the packet was received.

6.2.3.2.1 Registration

When the P-CSCF receives a REGISTER request from the UE that does not contain an Authorization header and does not contain a Security-Client header, the P-CSCF shall handle the Path header, the Require header, the P-Charging-Vector header and the P-Visited-Network-ID header as described in clause 5.2.12 of TS 24.229 [7]. Afterwards the P-CSCF shall determine the I-CSCF of the home network and forward the request to that I-CSCF.

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) handle the Service-Route header, the public user identities, the P-Asserted-Identity header, the P-Charging-Function-Address header as described in clause 5.2.2 of TS 24.229 [7] for the reception of a 200 (OK) response; and
2) forward the 200 (OK) response to the UE.
3) The P-CSCF shall support SIP compression as described in TS 24.229[7] subclause 8.2.1 with the exception that no security association exists between the UE and the P-CSCF. Therefore, when the P-CSCF creates the compartment is implementation specific.

6.2.3.2.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

As the early IMS security solution does not offer IPsec, the P-CSCF shall implement the procedures as described in clause 5.2.6 of TS 24.229 [7] with the following deviations.

For requests initiated by the UE, when the P-CSCF receives a 1xx or 2xx response, the P-CSCF shall not rewrite its own Record Route entry.

For requests terminated by the UE, when the P-CSCF receives a request, prior to forwarding the request, the P-CSCF shall not include a protected server port in the Record-Route header and in the Via header.

6.2.3.3 Procedures at the I-CSCF

Early IMS security requires that the I-CSCF between a P-CSCF and S-CSCF does not alter the Via header. An I-CSCF between an S-CSCF and another S-CSCF is unaffected by early IMS security.

~~NOTE:~~ Topology hiding is not available between a P-CSCF and a S-CSCF with early IMS security because ~~topology hiding~~it alters the Via header.

6.2.3.4 Procedures at the S-CSCF

6.2.3.4.1 Registration

Upon receipt of an initial REGISTER request without an Authorization header, the S-CSCF shall:

1) identify the user by the public user identity as received in the To header of the REGISTER request;
2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;
3) if no IP address is stored for the UE, query the HSS, as described in clause 6.2.5 with the public user ID as input and store the received IP address of the UE. Prior to contacting the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in TS 29.228 [10];

   NOTE: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

4) check whether a "received" parameter exists in the Via header field provided by the UE. If a "received" parameter exists, S-CSCF shall compare the IP address recorded in the “received” parameter against the UE's IP address stored during registration. If no "received" parameter exists in the Via header field provided by the UE, then S-CSCF shall compare IP address recorded in the "sent-by" parameter against the stored UE IP address. In both cases, if stored IP address and the IP address recorded in the Via header provided by the UE do not match, the S-CSCF shall query the HSS, as described in clause 6.2.5 with the public user ID as input and store the received IP address of the UE. If the stored IP address and the IP address recorded in the Via header provided by the UE still do not match the S-CSCF shall reject the registration with a 403 (Forbidden) response and skip the following steps.
5) handle the Cx Server Assignment procedure, the ICID, each non-barred registered public user identity, the Path header, the registration duration as described in clause 5.4.1.2.2 of TS 24.229 [7]; and send a 200 (OK) response to the UE as described in clause 5.4.1.2.2 of TS 24.229 [7].

6.2.3.4.2 General treatment for all dialogs and standalone transactions excluding REGISTER requests

On the reception of any request other than an initial REGISTER request, the S-CSCF shall check whether a "received" parameter exists in the Via header field provided by the UE. If a "received" parameter exists, S-CSCF shall compare the IP address received in the "received" parameter against the UE's IP address stored during registration. If no "received" parameter exists in the Via header field provided by the UE, then S-CSCF shall compare IP address received in the "sent-by" parameter against the IP address stored during registration. If the stored IP address and the IP address received in the Via header field provided by the UE do not match, the S-CSCF shall reject the request with a 403 (Forbidden) response. In case the stored IP address and the IP address receive in the Via header field provided by the UE do match, the S-CSCF shall proceed as described in clause 5.4.3 of TS 24.229 [7].

6.2.4 Identities and subscriptions

When early IMS security is supported, the HSS shall include for each subscription an IMPI and IMPU derived from the IMSI of the subscription according to the rules in TS 23.003 [8]. If the network supports both early IMS security and fully compliant IMS security, the IMSI-derived IMPI and IMPU shall be stored in addition to other IMPIs and IMPUs that may have been allocated to the subscription.

If a UE attempts a registration using early IMS security, the REGISTER shall include an IMPU that is derived from the IMSI that is used for bearer network access according to the rules in TS 23.003 [8]. The UE shall apply this rule even if a UICC containing an ISIM is present in the UE.

In the case that a UE is registering using early IMS security with an IMSI-derived IMPU, implicit registration shall be used as a mandatory function to register the subscriber's public user identity(s) using the rules defined in clause 5.2.1a.1 of TS 23.228 [3]. By applying these rules the IMSI-derived IMPU shall be barred in the HSS for all procedures other than SIP registration.

6.2.5 Impact on Cx Interface

Early IMS Security mechanism affects the use of the protocol defined for the Cx interface. In particular, the User-Authorisation-Request and Multimedia-Auth-Request/Answer messages are impacted.

Because in Early IMS Security the Private User Identity of the subscriber is not made available to the IMS domain in SIP messages, it is necessary to derive a Private User Identity from the Temporary Public User Identity to use as the content of the User-Name AVP in certain Cx messages (most notable UAR and MAR).

6.2.5.1 User registration status query

The UAR command, when implemented to support Early IMS Security follow the description in clause 6.1.1 of TS 29.228 [10], with the following exception:

- the Private User Identity (User-Name AVP) in the UAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present port number, URI parameters, and headers.

6.2.5.2 Authentication procedure

The MAR and MAA commands, when implemented to support Early IMS Security follow the description in clause 6.3 of TS 29.228 [10], with the following exceptions:

- the Private User Identity (User-Name AVP) in the MAR command shall be derived from the temporary Public User Identity URI being registered by removing URI scheme and the following parts of the URI if present: port number, URI parameters, and headers.
- In the MAR and MAA commands, the Authentication Scheme (Authentication-Scheme AVP described in clause 7.9.2 of TS 29.228 [10]) within the SIP-Auth-Data-Item grouped AVP shall contain "Early-IMS-Security".
- In the MAA command, the SIP-Auth-Data-Item grouped AVP shall contain the user IP address. If the address is IPv4 it shall be included within the Framed-IP-Address AVP as defined in draft-ietf-aaa-diameter-nasreq-17.txt [11]. If the address is IPv6 it shall be included within the Framed-IPv6-Prefix AVP and, if the Framed-IPv6-Prefix AVP alone is not unique for the user it shall also contain Framed-Interface-Id AVP.
  This results in SIP-Auth-Data-Item as depicted in table 6.3.4 of TS 29.228 [10], being replaced when Early IMS Security is employed by a structure as shown in table 2.

Table 2: Authentication Data content for Early IMS Security

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For Early IMS Security it will indicate "Early-IMS-Security"
User IPv4 Address	Framed-IP-Address	C	If the IP Address of the User is an IPv4 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].
User IPv6 Prefix	Framed-IPv6-Prefix	C	If the IP Address of the User is an IPv6 address, this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].
Framed Interface Id	Framed-Interface-Id	C	If the IP Address of the User is an IPv6 address and the Framed-IPv6-Address AVP alone is not unique for the user this AVP shall be included. For a description of the AVP see draft-ietf-aaa-diameter-nasreq-17.txt [11].

The ABNF description of the AVP as given in clause 6.3.13 of TS 29.229 [12] is replaced with that given below.

```
SIP-Auth-Data-Item :: = < AVP Header : TBD >
   [ SIP-Authentication-Scheme ]

   [ Framed-IP-Address ]

   [ Framed-IPv6-Prefix ]

   [ Framed-Interface-Id ]

   * [AVP]
```

- Step 5 of clause 6.3.1 of TS 29.229 [12] shall apply with the following exception:
  - HSS shall return only one SIP-Auth-Data-Item

6.2.6 Interworking cases

For the purposes of the interworking considerations in this clause, it is assumed that the IMS entities P-CSCF, I-CSCF, S-CSCF and HSS reside in the home network and all support the same variants of IMS, i.e. all support either only early IMS security, or only fully compliant IMS security, or both.

NOTE: It is compatible with the considerations in this document that the UE uses different APNs to indicate the IMS variant currently used by the UE, in case the P-CSCF functionality is split over several physical entities.

It is expected that both fully compliant UEs implementing the security mechanisms in TS 33.203 [2] (denoted "fully compliant IMS security" in the following) and UEs implementing the early IMS security solution specified in the present document (denoted "early IMS security" in the following) will access the same IMS. In addition, IMS networks will support only fully compliant IMS UEs, early IMS UEs, or both. Both UEs and IMS networks must therefore be able to properly handle the different possible interworking cases.

Since early IMS security does not require the security headers specified for fully compliant IMS UEs, these headers shall not be used for ~~early IMS~~early IMS security. The REGISTER request sent by an ~~early IMS~~early IMS security UE to the IMS network shall not contain the security headers specified by TS 33.203 (Authorization and Security-Client).

As a result, ~~early IMS~~early IMS security UEs shall not add an explicit indication for the security used to the IMS signaling.

An IMS network supporting both early IMS security and fully 3GPP compliant IMS security UEs shall use early IMS security for authenticating the UE during registrations that do not contain the security headers specified by TS 33.203 (Authorization and Security-Client).

Without sending an Authorization Header in the initial REGISTER request, early IMS UEs only provide the IMS public identity (IMPU), but not the IMS private identity (IMPI) to the network (this is only present in the Authorization header for fully compliant IMS security UEs).

During the process of user registration for early IMS security, the Cx interface carries only the public user identity in Cx-MAR requests (sent by I-CSCF and S-CSCF HSS). The private user identity within these requests shall contain the IMPU as received by the UE. This avoids changes to the message format on the Cx interface.

If the S-CSCF receives an indication that the UE is an early IMS UE, then it shall be able to select the "Early-IMS-Security" authentication scheme in the Cx-MAR request. The Cx interface shall support the error case that the S-CSCF selects the "Digest-AKAv1-MD5" authentication scheme based on UE indication, but the HSS detects that the subscriber has a SIM instead of a USIM or ISIM. In this case the HSS shall respond with an appropriate error command. The S-CSCF will then respond to the UE with a 403 (Forbidden) response. If the UE is capable of early IMS security then, according to step 5, the UE will take this as an indication to attempt registration using early IMS security.

For interworking between early IMS security and fully compliant IMS security implementations during IMS registration, the following cases shall be supported:

1. Both UE and IMS network support early IMS security only
   IMS registration shall take place as described by the present document.
2. UE supports early IMS security only, IMS network supports both early IMS security and fully compliant IMS ~~access~~ security
   Early IMS security according to this annex shall be used for authenticating the UE for all registrations from UEs that do not provide the fully compliant IMS security headers.
3. UE supports both, IMS network supports early IMS security only
   If the UE already has knowledge about the IMS network capabilities (which could for example be preconfigured in the UE), the appropriate authentication method shall be chosen. The UE shall use fully compliant IMS security, if the network supports this, otherwise the UE shall use early IMS security.
   If the UE does not have such knowledge it shall start with the fully compliant IMS Registration procedure. The early IMS P-CSCF shall answer with a 420 (Bad Extension) failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial REGISTER request.

   NOTE: The Proxy-Require header cannot be ignored by the P-CSCF.

   The UE shall, after receiving the error response, send an early IMS registration, i.e., shall send a new REGISTER request without the fully compliant IMS security headers.
4. UE and IMS network support both
   The UE shall start with the fully compliant IMS security registration procedure. The network, with receiving the initial REGISTER request, receives indication that the IMS UE is fully compliant and shall continue as specified by TS 33.203 [2].
5. Mobile equipment and IMS network support both, UE contains a SIM
   The UE might start with the fully compliant IMS security registration procedure. However, when the S-CSCF requests authentication vectors from the HSS, the HSS will discover that the UE contains a SIM and return an error.
   The S-CSCF shall answer with a 401 (Unauthorized) with an Error-info: header containing the text "Early security required". The UE then retries using early IMS security.
6. UE supports early IMS security only, IMS network supports fully compliant IMS ~~access~~ security only

The UE sends a REGISTER request to the IMS network that does not contain the security headers required by fully compliant IMS security. The fully compliant IMS security P-CSCF will detect that the Security-Client header is missing and return a 4xx responses, as described in clause 5.2.2 of TS 24.229 [7].

7. UE supports fully compliant IMS ~~access~~ security only, IMS network supports early IMS security only
The UE shall start with the fully compliant IMS security registration procedure. The early IMS P-CSCF shall answer with a 420 (Bad Extension) failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial REGISTER request. After receiving the error response, the UE shall stop the attempt to register with this network, since the fully compliant IMS security according to TS 33.203 [2] is not supported.

6.2.7 Message flows

6.2.7.1 Successful registration

Figure 1 below describes the message flow for successful registration to the IMS that is specified by the early IMS security solution.

NOTE: The "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 6.2.3.2.

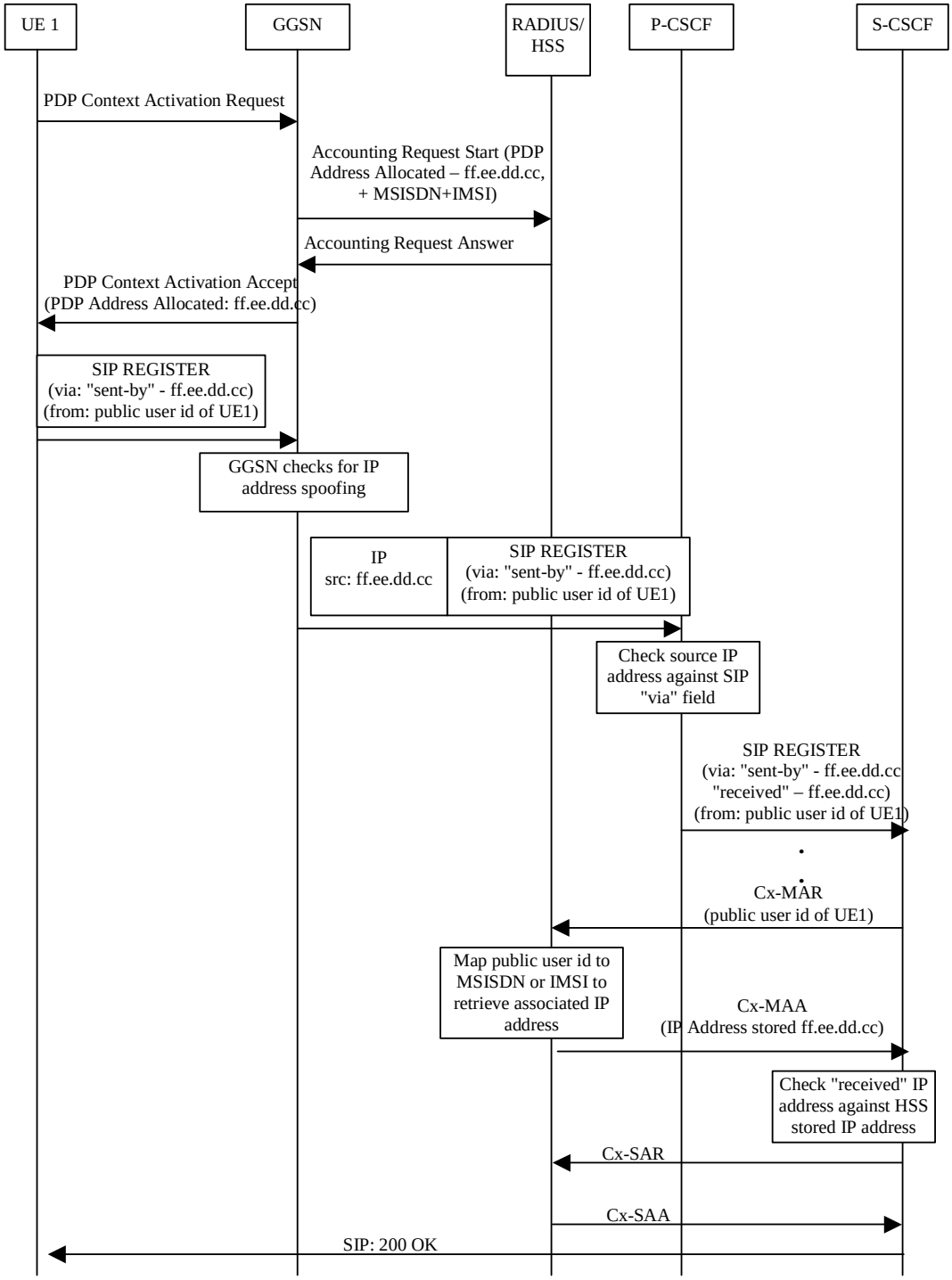

Figure 1: Message sequence for early IMS security showing a successful registration

6.2.7.2 Unsuccessful registration

Figure 2 below gives an example message flow for the unsuccessful attempt of an attacker trying to spoof the IMS identity of a valid IMS user.
Again, the "received" parameter is only present between P-CSCF to S-CSCF under the conditions given in clause 6.2.3.2.

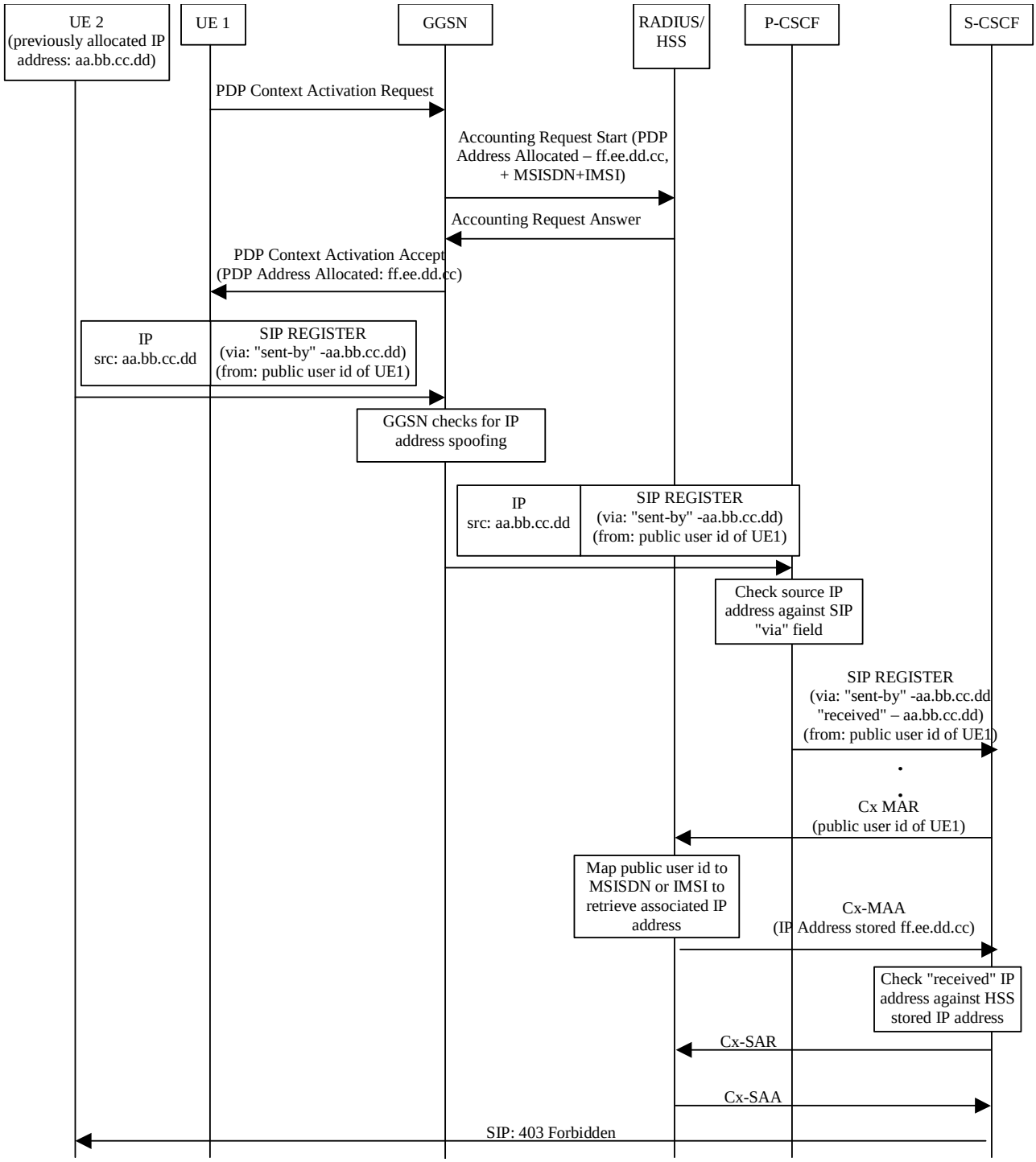

Figure 2: Message sequence for early IMS security showing an unsuccessful identity theft

6.2.7.3 Successful registration for a selected interworking case

Figure 3 below describes the message flow for successful registration to the IMS in the case that the UE supports both fully compliant IMS and early IMS access security and the network supports early IMS security only. This case is denoted as case 3 in clause 6.2.6.

NOTE: The "received" parameter is only sent from P-CSCF to S-CSCF under the conditions given in clause 6.2.3.2.

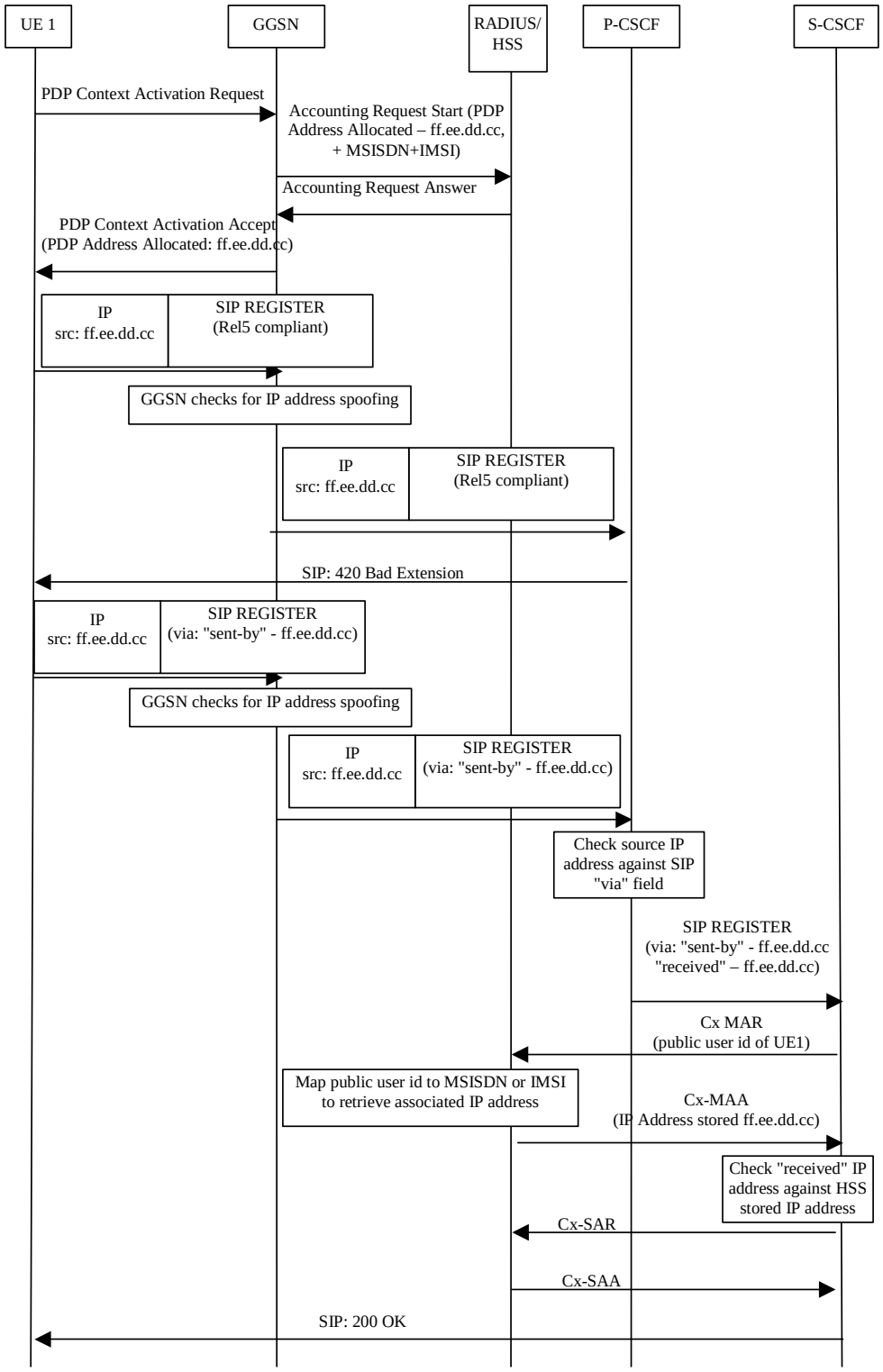

Figure 3: Message sequence for early IMS security showing interworking case where UE supports both fully compliant IMS and early IMS access security and network supports early IMS security only

Annex A:
Comparison with an alternative approach - HTTP Digest

An alternative approach would have been to use password-based authentication for early IMS implementations. For example, HTTP Digest (IETF RFC 2617) could have been used for authenticating the IMS subscriber. The HTTP Digest method is a widely supported authentication mechanism. It is not dependent of the GPRS network and it does not require new functional elements or interfaces in IMS network. However, this method would have required a subscriber-specific password to be provisioned on the IMS UE. This alternative is not adopted for use in early IMS systems.
The HTTP Digest method has the following advantages and disadvantages:
Advantages:

- Fully standardized and supported by RFC 3261 [6] compliant implementations and therefore by TS 24.229 [7] compliant implementations (SIP protocol mandates support of HTTP Digest).
- HTTP Digest can support partial message integrity protection for those parts of the message used in the calculation of the WWW-Authenticate and Authorization header field response directive values (when qop=auth-int).
- HTTP Digest implementations can employ methods to protect against replay attacks (e.g. using server created nonce values based on user ID, time-stamp, private server key, or using one-time nonce values).

Disadvantages:

- HTTP Digest may impose restrictions on the type of charging schemes that can be adopted by an operator. In particular, if a subscriber could find out his or her own password from an insecure implementation on the UE, then he or she could share the IMS subscription with friends. This could impact revenue for the operator if bundled or partly subscription based tariffs are used rather than purely usage based tariffs. For example, a subscriber could take out a subscription for 100 instant messages and then share this with his or her friends. Although contractual obligations could be imposed on customers to prohibit this behaviour, in practice this would be difficult to enforce without employing special protection mechanisms, e.g. disallow multiple binding to a single IP address. If charging were purely usage based then there would be no incentive for the subscriber to do this, therefore using HTTP Digest may not impact on operator's revenue. The solution specified in clause 6 is flexible in allowing a range of different charging models including bundled or partly subscription based tariffs.
- HTTP Digest provides a weaker form of subscriber authentication when compared with the levels of authentication used for other services offered over 3GPP networks, where authentication is typically based directly or indirectly on the (U)SIM. Subscription authentication depends, among other things, on the strength of the password used as well as on the password provisioning methods, such as bootstrapping passwords into the IMS capable UE. A weak subscriber authentication, vulnerable to dictionary attacks, has implications on the reliability of charging, and on the level of assurance that can be given to the customer that their communications cannot be masqueraded. In the solution specified in clause 6, authentication of the IMS subscriber is indirectly based on (U)SIM authentication at the GPRS level. The level of security is similar to that currently used for certain WAP services, where the user's MSISDN is provided by the GGSN to the WAP gateway. Security does not rely on the UE securely storing any long-term secret information (e.g. passwords).
- HTTP Digest provisioning is more complex since subscriber-specific information (i.e. passwords) must be installed or bootstrapped into each IMS UE.

3GPP TSG-CN1 Meeting #37 Tdoc N1-050278
Sydney, Australia, 14-18 February 2005

Title: LS on provisioning of the UE RAC and START_PS to the network

Response to: LS (GP-050575/ N1-050097) on method for provisioning of the UE RAC and START_PS to the network.

Release: Rel-6

Work Item: Support of Conversational Services in A/Gb Mode via the PS Domain

Source: CN1

To: GERAN2, RAN2, RAN3

Cc: ---

Contact Person:
Name: Robert Zaus
E-mail Address: robert.zaus@siemens.com

Attachments: N1-050404 [CR 24.008 – 950 rev2; agreed by CN1].

---

1. Overall Description:

CN1 would like to thank GERAN 2 for the liaison statement on Method for provisioning of the UE RAC and START_PS to the network (GP-050575/ N1-050097).

CN1 have considered the methods proposed by GERAN 2 for providing the parameters UE RAC and START PS to the network and have agreed the attached CR to TS 24.008. The agreed method deviates from the example CR sent by GERAN 2 in a few points:

i) The information is sent by the mobile station during the GPRS attach or routing area update procedure, when the SGSN explicitly requests the mobile station in the Attach Accept or Routing Area Update Accept message to do so. Accordingly, the information will be included by the MS in the **Attach Complete** or **Routing Area Update Complete** message. – This allows some optimizations at the radio interface, e.g. the SGSN need not request the information during each intra-SGSN routing area update.

ii) The parameters UE RAC and START_PS will be transmitted in a new information element "Inter RAT information container". This is an information element of variable length, with a minimum length of 3 and a **maximum length of 40 octets**. – CN1 considered it appropriate to define a fixed maximum length, since the information needs to be stored by the SGSN potentially for each subscriber registered with the SGSN.

When setting an upper limit of 40 octets, corresponding to a value part of 38 octets, CN1 made the assumption that the MS would include only one of the two parameters "Predefined configuration status information" and "Predefined configuration status information compressed", and only one of the two parameters "UE radio access capability" and "UE radio access capability compressed" in the INTER RAT HANDOVER INFO (see TS 25.331, subclause 10.2.16d). Since the compressed encoding was introduced in Rel-5 and PS Inter-RAT Handover is a Rel-6 feature, CN1 further assumed that all RNCs supporting PS Inter-RAT Handover would be able to decode the compressed format of the parameters.

1. CN1 kindly ask **RAN2** to check whether these assumptions are correct and whether 38 octets are sufficient to store the necessary UE RAC and START_PS information.

2. CN1 also ask **RAN2** to indicate whether it is correct that the INTER RAT HANDOVER INFO from TS 25.331, subclause 10.2.16d) is the information to be included in the "Inter RAT information container" in TS 24.008.

Concerning the transport of the UE RAC and START_PS information to the target RNC during a GERAN to UTRAN inter-RAT PS handover, CN1 would like to make the following proposal to **GERAN 2** and **RAN3**:

- Since the SGSN needs to store this information anyway, and
- the serving BSC will forget the information each time the packet flow context is released, and
- the information is sent to the BSC only for the purpose to be sent back via the SGSN to the target RNC,

CN1 would like to propose that the information is treated by the SGSN in the following way:
The information is stored in the SGSN and never sent to the serving BSC. At inter-system handover from GERAN to UTRAN, the SGSN includes the information as RANAP parameter in the RANAP Relocation Request message to the target RNC.

This would allow to avoid unnecessary transmissions and re-transmissions of the UE RAC and START_PS information via the Gb interface.

Please note that the same handling is already used for the transport of the UMTS Ciphering Key and Integrity Key to the target RNC during circuit-switched inter-system handover from GERAN to UTRAN.

If CN1's proposal is adopted, GERAN 2 would probably need to specify a mechanism how the serving BSC can determine whether the SGSN supports PS inter-system handover from GERAN to UTRAN (e.g. by local administration in the BSC or by BSSGP signalling between BSC and SGSN).

2. Actions:

To GERAN 2, RAN2, RAN3 group.

ACTION:

CN1 asks **GERAN2**:
to note the attached CR.

CN1 asks **RAN2**:
to answer CN1's questions and to confirm that the size of the "Inter RAT information container" is sufficient.

CN1 asks **GERAN2 and RAN3**:
to take CN1's proposal for the transport of the UE RAC and START_PS information from the SGSN to the target RNC into account.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050406
Sydney, Australia, 14-18 February 2005

Title: Reply LS (to G2-0402911) on the PS Handover Work
Response to: LS (N1-041977/G2-0402911) on "the PS Handover Work"
Release: Rel-6
Work Item: SCSAGB
Source: CN1
To: GERAN
Cc: SA2, RAN2, RAN3, CN4

Contact Person:
Name: Christian Herrero
Tel. Number: +46 46231812
E-mail Address: christian.herrero@ericsson.com

Attachments: None

---

1. Overall Description:

CN1 would like to inform GERAN that it has reviewed the Stage 2 specification 3GPP TS 43.129 v6.0.0 on 'Packet-Switched handover for GERAN A/Gb mode'.

CN1 has studied the 3GPP TS 43.129 and CN1 has taken note that the current version of 3GPP TS 43.129 does not reuse the legacy core-network procedures, but impacts all layers above the RR-sublayer. Certainly, new error cases will be created by newly defined procedures. Furthermore, extensive updates in terminals are required.

Alternative proposals to simplify the impacts on core-network protocols have been proposed at CN1#37. Additionally, a set of CRs has been provided for information aiming at fulfilling the requirements outlined in 3GPP TS 43.129 in an alternative way. These CRs include proposals to minimize core-network protocol impacts by re-using existing mechanisms, e.g. the XID Command – XID Response and SABM-UA procedures, to a larger extent than foreseen by 3GPP TS 43.129.

CN1 will investigate this further and one company has volunteered to try to complete the CN1 work related to the PS Handover feature within Rel-6 at next meetings.

2. Actions:

To GERAN group.

ACTION: CN1 kindly requests to take note of the points raised above and invites for further comments.

3. Date of Next TSG-CN1 Meetings:

CN1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050407
Sydney, Australia, 14-18 February 2005

Title: Reply LS (to R2-042734 and S2-050488) on NAS signalling load at MBMS Session Start/Stop

Response to: LS (N1-050018/R2-042734 and N1-050260/S2-050488) on "NAS signalling load at MBMS Session Start/Stop"

Release: Rel-6

Work Item: MBMS

Source: CN1, SA2

To: RAN2

Cc: SA1, SA2, RAN3, GERAN2

Contact Person:
Name: Christian Herrero
Tel. Number: +46 46231812
E-mail Address: christian.herrero@ericsson.com

Attachments: None

---

1. Overall Description:

CN1 thanks RAN2 for their LS on NAS signalling load at MBMS Session Start/Stop. CN1 would like to provide feedback on the following actions:

2) RAN2 request feedback from SA2 and CN1 on whether there are any NAS level mechanisms to restrict the number of UEs that initiate NAS signalling simultaneously due to non-MBMS service activation/re-activation or de-activation,

CN1 would like to inform RAN2 that it has not been defined any core-network protocol mechanism to restrict UEs of performing activation/de-activation of non-MBMS services when an MBMS Session start/stop occurs.

Additionally, the CN1 MBMS-related Stage 3 specification does not require the UE to de-activate PDP contexts when receiving an MBMS Notification of the immediate start of an MBMS session. Therefore, CN1 has agreed that the following statements seem to be overestimated:
"On receiving MBMS Notification immediately following MBMS session start, a high number of UEs may access the network in order to de-activate ongoing non-MBMS services"
"Respectively at MBMS session stop, a high number of UEs may access the network in order to activate/re-activate non-MBMS services (especially in the PS domain)"

At present, CN1 specifications do not contain any requirement on activation and de-activation of non-MBMS GPRS services (PDP contexts) at MBMS Session start/stop. This is implementation dependent and it relates to the maximum capabilities of a specific UE implementation is capable of (e.g. some UEs may be able to handle simultaneously one MBMS session and one or more PDP contexts of different traffic classes).

3) RAN2 request feedback from SA2 and CN1 on whether they expect AS level mechanisms to be used to reduce peak SGSN load during MBMS counting.

CN1 has discussed the question asked by RAN2 and CN1 assumes that there will be in place an AS level mechanism to reduce the SGSN load because of the MBMS counting procedure.

2. Actions:

To RAN2, SA2 group.

ACTION: CN1 kindly requests RAN2 and SA2 to take note of the above answers.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050408
Sydney, Australia, 14-18 February 2004

Title: LS on Early IMS Security TR 33.878
Response to: LS (N1-041673) on Security aspects of early IMS systems from SA3
Release: Rel-6
Work Item: FS on Security for early IMS (SEC-IMS)

Source: CN1
To: SA3
Cc:

Contact Person:
Name: Peter Dawes
Tel. Number: +44 7717 275009
E-mail Address: peter.dawes@vodafone.com

Attachments: N1-050403

---

1. Overall Description:

In TSG SA-26, CN1 was asked to review TR 33.878 v1.0.0 on "Security Aspects of Early IMS", check the the impact on the full-solution IMS and provide any comments to SA WG3. The TSG CN Chairman reported that CN WG1 requirements and concerns were expected to be documented in this TR, rather than as CRs to the main specification.

Several contributions were brought to CN1#37, but it was found that the solution in TR 33.878 was too far advanced to allow any significant stage 3 changes by CN1. CN1 could provide a more effective review if involved earlier in similar work in the future.

CN1 reviewed TR 33.878 during meeting CN1#37 and the suggested changes can be summarized as follows:

- Some text was considered too strongly normative for a TR and has been re-worded.
- The dependency and relationship between early IMS security and the IP version is clarified.
- The IMS features and requirements that are turned off or downgraded in early IMS security have been collected in a single subclause of the TR.
- In particular, restrictions on registering public user identities have been clarified.
- The wording in the TR has been systematically edited to indicate that it applies to early IMS security only.
- Restrictions on the use of I-CSCFs have been clarified, particularly that I-CSCFs between S-CSCFs are unaffected by the TR.
- The relationship between the early IMS security and creation of compartments for SIP compression using SigComp has been clarified.

Suggested changes are attached to this liaison statement.

2. Actions:

To SA3 group.

ACTION:

CN1 kindly requests that SA3 consider the changes proposed in document N1-050403 attached to this liaison statement.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th -29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050410
Sydney, Australia, 14-18 February 2005

Title: LS on service based inter-system hand over
Response to: None
Release: Rel-6
Work Item: TEI

Source: CN1
To: SA1, SA2, GERAN2
Cc: CN3

Contact Person:
Name: Pierre-Jean Muller
Tel. Number: +33 149072814
E-mail Address: pierre-jean.muller@nectech.fr

Attachments: N1-050398 (its status is postponed to the next meeting CN1#38)

---

1. Overall Description:

CN1 would like to draw SA1, SA2 and GERAN2 attention to the following protocol enhancement:

In the current specifications, it is possible for the network to hand-over a dual mode GSM/UMTS UE to another RAT based on the requested services or based on radio conditions at call set up or during an ongoing call.

However the current specifications do not define the case where a dual mode GSM/UMTS UE that supports transparent bearer services (e.g. CS multimedia) in UMTS but not in GSM, is attached in a GSM radio network and wants to set up such call in UMTS.

It is CN1's understanding that stage 1 requirement covers already such protocol enhancement (see TS 22.129 “Handover requirement between UTRAN and GERAN” clause 5.2.).

As per and limited to the proposed solution presented in CN1 (see the attached document N1-0500398):

- It is CN1's understanding that there is no impact on stage 2 specifications with the possible exception of TS 23.009 “Handover procedure”. This stage 2 specification is actually under CN1 responsibility and therefore changes can be handle within CN1 WG.
- It is CN1's understanding that there is no impact on GERAN or RAN stage 3 specifications.

Nevertheless CN1 is not sure whether this protocol enhancement needs further stage 2 consideration or has dependency with other features like SCUDIF or “Redial solution for voice-video switching”.

Along with the proposed solution CN1 did consider whether there is a need to be able to inhibit a dual mode UE from requesting bearer services that are not supported on the RAT the UE is camping on (i.e. GSM) and cannot be handed over to the other RAT ‘(i.e. UMTS). For example because of no UMTS coverage or because the network does not supports GSM to UMTS handover. In this way we avoid unnecessary signalling towards and from the network, unnecessary reject calls and finally improve user experience by preventing the user from attempting to setup such calls when or where the network is not able to successfully proceed the call on the other RAT. It should be possible to inform the UE whether the network supports or not such service by adding an indication in the system information broadcasted by the GSM cell. The drawback of this solution is we create a dependency with the radio access network. Other options are not excluded.

Furthermore CN1 did consider a potential alternative solution based on Mobile Station Classmark 3 (see TS 24.008 clause 10.5.1.7) and service-based handover (see TS 23.009 clause 14) but this option has not been studied in detailed.

2. Actions:

To SA1:

1. CN1 kindly asks SA1 whether the proposed UE request for service based handover (N1-050398) is in line with stage 1 requirements.
2. If SA1 agreed question 1 do they consider such requirement to cover as well in-call modification case.
3. Based on the proposed solution, CN1 kindly asks SA1 whether a mechanism to inhibit a UE as mentioned by CN1 shall be provided.

To SA2 and GERAN2

4. CN1 kindly asks SA2 and GERAN2 whether the proposed change (N1-050398) is in line with actual stage 2 specifications and GERAN stage 3 specifications.
5. CN1 welcomes any additional guidance from SA2 and GERAN2 regarding the statements and assumptions provided above.

3. Date of Next TSG-CN1 Meetings:

CT1_38	25th - 29th April 2005	Cancun, Mexico

3GPP TSG-CN1 Meeting #37 Tdoc N1-050415
Sydney, Australia, 14-18 February 2005

Title: Reply LS on LS on protocol aspects for CSI
Response to: LS on protocol aspects for CSI
Release: Rel-6 and Rel-7
Work Item: CSI

Source: CN1
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:

CN1 thanks SA2 for their LS on protocol aspects for CSI. CN1 would like to inform SA2 that they have agreed a Work Item for the stage 3 protocol work on CSI.

CN1 has briefly discussed the questions from SA2 however there was insufficient background information provided for CN1 to fully analyse the questions and provide definitive responses to all these questions.

CN1 provides the following provisional responses to the questions:

- *Is the SIP OPTIONS request and/or response able to carry (end-to-end between UEs) both an IMS Public User Identity in the form of an SIP URI and the MSISDN of the UE in the form of a TEL URI simultaneously?*
- An OPTIONS request/response can contain multiple Contact headers, but currently there is no way to indicate whether a number is MSISDN or to be used with SIP. Also note that if the OPTIONS request is forked in the network the calling UE will receive only one response, i.e. it will get aware of the capabilities of only one of the UEs which received the OPTIONS request.

- *If yes, how would a Rel-6 UE interpret a TEL URI in e.g. the contact header of an OPTIONS request and response?*
- TEL URI indicates a point of contact, but doesn't state which protocol to use. Also, while Contact can be used in OPTIONS, it has no defined meaning, and the meaning could be different whether the OPTIONS is sent within or outside an existing dialog.

- *Is the SIP INVITE request and/or response able to carry (end-to-end between UEs) both an IMS Public User Identity in the form of an SIP URI and the MSISDN of the UE in the form of a TEL URI simultaneously?*
- No. An INVITE can only contain one Contact header, and that is used for SIP routing subsequent requests.

- *For optimisation reasons SA2 are considering whether it is possible to include an SDP body in an SIP OPTIONS request. If included, what type of behaviour can be expected from a UAS receiving such a request?*
- An options request may contain a body, however the use of an SDP body with an options request is undefined. SIP must use the offer answer model with SDP as specified in RFC3264. It is hard to see how the semantics of OPTIONS fit with the semantics of offer answer especially since the response to an OPTIONS request is specified to contain SDP representing the full set of media capabilities if the Accept header contains an “Application/SDP” value.

- *SA2 would like to understand the practicalities, process, and timeframe for defining new 3GPP-specific Caller Preference feature tags. SA2 would welcome CN1's clarification on this matter.*
- CN1 has no experience from defining a Caller Preference feature tag, but assumes that if IANA registration is needed, this is possible within weeks. It should be considered whether such feature tag would require an IETF RFC to be defined, or if proprietary tag can be used. See RFC 2506 Media Feature Tag Registration Procedure

- *SA2 would like to ask whether an implicit mechanism could be used to indicate whether a UE supports a specific service such as CS and IMS combinational services?*
- Implicit indication may always cause problems (e.g. due to forking) and explicit indications are safer but have currently not been specified for the services mentioned above, whatever they may be.

CN1 would like to point out that it is impossible to give a tutorial on the mechanisms available to extend SIP in a single liaison statement, and would welcome requirements on which to base the protocol design rather than protocol proposals.

2. Actions:

CN1 asks SA2 to take the answers into account for their stage 2 level work, but also to supply CN1 with the background information and requirements necessary for CN1 to make appropriate protocol decisions to implement the stage 3 parts of CSI.

3. Date of Next TSG-CN1 Meetings:

CT1 #38	25th – 29th of April 2005	Cancun, Mexico
CT1 #39	15th – 19th of August 2005	TBD

3GPP TSG-CN1 Meeting #37 Tdoc N1-050416
Sydney, Australia, 14-18 February 2005

Title: LS on status of 3GPP IMS management object
Response to:
Release: Rel-6
Work Item: IMS2

Source: 3GPP TSG CN1
To: OMA PAG, OMA POC, OMA DM, 3GPP2 TSG-X
Cc: 3GPP TSG CN

Contact Person:
Name: Andrew Allen
Tel. Number: +1 847 809 8636
E-mail Address: aallen@rim.com

Attachments: TS 24.167 v.2.0.0 3GPP IMS Management Object (MO)

---

1. Overall Description:

CN1 would like to inform OMA and 3GPP2 that it has now completed its work on TS 24.167, the technical specification for the 3GPP IMS management object and will present it to TSG CN for approval and inclusion in 3GPP release 6 as version 6.0.0 at the March 2005 TSG CN meeting.

CN1 would also like to inform OMA that 3GPP has documented as part of the work on early IMS security how the private user identity, public user identity and home network domain name are obtained when using a 2G SIM.

2. Actions:

To OMA PAG / OMA POC / OMA DM

ACTION: OMA PAG, OMA POC and OMA DM are invited to comment back to CN1 any issues, concerns or additional requirements they may have for the IMS MO.

To 3GPP2 TSG-X

ACTION: CN1 would like 3GPP2 to take note of the status of the work on the 3GPP IMS MO.

3. Date of Next TSG-CN1 Meetings:

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