3GPP TSG CN Plenary Meeting #16 **NP-020215**
5th - 7th June 2002. Marco Island, USA.

Source: **MCC**

Title: **All LSs sent from CN1 since TSG CN#15 meeting,- pack 2**

Agenda item: **6.1.1**

Document for: **INFORMATION**

Introduction:

This document contains **7 agreed** LSs sent from **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #15 for information only.

Meeting	TDoc #	Status	Source	Tdoc Title	Type	Comments
N1-SIPadhoc 0204	N1-021084	AGREED	Keith	Liaison Statement on discovery and subsequent request of specific capabilities within the MRFC/MRFP (and discovery of specific capabilies within the MGCF/MGW)	LS OUT	Related to 985. To: SA2
N1-24	N1-021364	AGREED	Hannu	Liaison Statement on UE behaviour when network fails authentication	LS OUT	Linked to 0683. To: RAN2
N1-24	N1-021365	AGREED	Roland	Response LS on "Alternative coding of the MS RAC IE"	LS OUT	Linked to 1117. To: GERAN2
N1-24	N1-021427	AGREED	A. Allen	Response LS to SA2 on IMS Identities for Rel 99/R4 UICC	LS OUT	Related to 1250. To: SA1, SA2, Cc: SA3, CN4, T3
N1-24	N1-021446	AGREED	Duncan	Liaison Statement on Deriving IMS parameters from a Pre-Release 5 UICC	LS OUT	To: CN4
N1-24	N1-021455	AGREED	Sunil	Liaison Statement on 3GPP Network Domain Name usage for IMS	LS OUT	To: GSMA SerG, GSMA IREG, Cc: CN4, SA2, CN
N1-24	N1-021477	AGREED	Jeremy/Nortel	Terminal determination of network support of EDGE	LS OUT	Related to 1208, To: GERAN, SA1

3GPP TSG-CN1 Meeting #SIPadhoc0204 ***Tdoc N1-021084***

Madrid, Spain, 23. – 25. April 2002

Title: Liaison Statement on discovery and subsequent request of specific capabilities within the MRFC/MRFP (and discovery of specific capabilies within the MGCF/MGW)

Source: CN1

To: SA2

Cc:

Contact Person:

Name: Keith Drage

Tel. Number: +44 1793 776249

E-mail Address: drage@lucent.com

Attachments: N1-020985

---

1. Overall Description:

3GPP Working Group CN1 has received a number of contributions relating to the provision of signalling functionality between the Application Server and the MRFC. The assumption in these contributions is that such requests are made from AS to S-CSCF over the ISC interface, and the S-CSCF subsequently makes requests over the Mr reference point.

The proposed discussion is reflected in the attachment to this liaison statement (N1-020985) and may be summarised as the following:

1. Does Rel-5 include support for basic call scenarios for tones, announcements, transcoding, and conference calls. This includes a description of how to pass instructions for the requested function using XML within the message body (or any other protocol solution).
2. Does Rel-5 include support for the OPTIONS request to return MRFC (and MGCF) capabilities to the AS.
3. Does Rel-5 include support for optimising the signalling when tones/announcements are needed for existing session that it is using and MRFP (or MGW), assuming that the same MRFP (or MGW) gets used for playing the tone/announcement.
4. Does Rel-5 require an option of having AS send a request using a generic MRFC request URI. However, this may be need to be deferred to Rel-6 to utilize an IETF based solution with Request URI parameters.

CRs for one method of supporting these requirements have been contributed, but confirmation is required from SA2 as to whether the requirements for all or any of the above exist within Release 5, before proceeding with any selection and documentation of a protocol solution.

In a similar manner, it may be advantageous for an MGCF to respond to an OPTIONS request with a similar list of supported capabilities of the MGW, and it would be desirable to know if this is also a requirement within release 5. If required, a similar protocol solution to that for the MRFC could be adopted.

2. Actions:

To SA2 group.

ACTION: CN1 asks if the above described functionality is accommodated within the requirements of 3GPP TS 23.002 and 3GPP TS 23.228 Release 5, or if such functionality is deferred until later releases, or not required at all.

3. Date of Next CN1 Meetings:

CN1_24	13th – 17th May 2002	Budapest, Hungary
CN1_25	29th July – 2nd August 2002	Helsinki, Finland

3GPP TSG-CN1 Meeting #24 **Tdoc N1-021364**
Budapest, Hungary, 13. – 17. May 2002

Title:	Liaison Statement on UE behaviour when network fails authentication
Source:	CN1
To:	RAN2
Cc:	
Response to:	LS (R2-020596 / N1-020683) on **UE behaviour when network fails authentication** from RAN2.

Contact Person:

Name:	Hannu Hietalahti
Tel. Number:	+358 40 5021724
E-mail Address:	**hannu.hietalahti@nokia.com**

Attachments: N1-021389, N1-021390, N1-021278 [R99, Rel-4 and Rel-5 CR on 24.008]

---

1. Overall Description:

CN1 thanks RAN2 for their LS asking for clarification to UE actions when network fails authentication. The attached CRs on this issue were agreed during CN1 #24.

2. Actions:

To [RAN2] group.

ACTION:

None.

3. Date of Next CN1 Meetings:

CN1_25	29th July – 2nd August 2002	Helsinki, Finland
CN1_26	23rd – 27th September 2002	?, USA

3GPP TSG-CN1 Meeting #24 **Tdoc N1-021365**
Budapest, Hungary, 13. – 17. May 2002

Title:	**Response LS on "Alternative coding of the MS RAC IE"**
Source:	CN1
To:	GERAN WG2
Cc:	
Response to:	LS from GERAN in GP-021290 (N1-021117)

Contact Person:

Name:	Roland Gruber
E-mail Address:	roland.gruber@mch.siemens.de
Tel. Number:	+49 89 722 46392

Attachments:	N1-021396 24.008 R99	CR 637 r1 "Alternative coding of radio access capabilities"
	N1-021397 24.008 REL4	CR 638 r1 "Alternative coding of radio access capabilities"
	N1-021398 24.008 REL5	CR 639 r1 "Alternative coding of radio access capabilities"

---

1. Overall Description:

CN1 thanks GERAN for their LS on "Alternative coding of the MS RAC IE" in GP-021290 (N1-021117). CN1 has reviewed the attached CR on TS 24.008 and has agreed several additional minor corrections to the draft version provided by GERAN. The changes are marked with yellow in the attached R99 version of the CRs.

The CRs agreed by CN1 are attached for information.

2. Actions:

none

3. Date of Next CN1 Meetings:

CN1_25	29th July – 2nd August 2002	Helsinki, Finland
CN1_26	23rd – 27th September 2002	?, USA

3GPP TSG-CN1 Meeting #24 ***Tdoc N1-021427***

Budapest, Hungary 13-17. May 2002

Title:	Response Liaison Statement on IMS Identities for R99/R4 UICC
Source:	CN1
To:	SA1, SA2
Cc:	SA3, CN4, T3
Response to:	LS (S1-020871) on SA1 Assumptions on IMS identities and UICCs; and LS (S2-021526) on IMS Identities for Rel 99/R4 UICC from SA2.

Contact Person:

Name: Andrew Allen
Tel. Number: +1 972 473 5507
E-mail Address: aallen@dynamicsoft.com

Attachments: N4-020774, N1-021405, N1-021424, N1-021441

---

1. Overall Description:

CN1 thanks SA1 and SA2 on their Liaison Statements concerning the identity requirements for access to IMS with a R99/Rel-4 UICC.

CN1 would like to inform SA1 and SA2 that CN1 has approved CRs to IMS specifications TS 23.218 and TS 24.229 to implement the stage 2 requirements for Temporary Public User Identities and barred public user identities contained in the SA2 CRs to TS 23.228. CN1 has also discussed and agreed a CR to TS 23.003 that defines the format for the R99/Rel 4 UICC for Home Domain name, Private User Identity and Public User Identity based on the content of the discussion paper attached to the SA2 LS and forwarded this CR to CN4 where it was agreed as N4-020774.

CN1's understanding of CR 154 (S2-021525) and CR 155 (S2-021344) to TS 23.228 concerning barred public user identities is that services are never executed for session requests originated from or terminated to barred public user identities. The S-CSCF therefore will always return a 4XX response to any request (other than REGISTER) originated from or terminated to a barred public user identity before any match is made of triggers in the initial filter criteria. This means that an Application Server cannot be contacted for a session request from or to a barred public user identity.

2. Actions To SA2:

To confirm that the S-CSCF should always return a 4XX response to any request (other than REGISTER) originated from or terminated to a barred public user identity before any match is made of triggers in the initial filter criteria.

3. Date of Next CN1 Meetings:

CN1_25	29th July – 02nd August 2002	Helsinki, Finland

3GPP TSG-CN1 Meeting #24 **Tdoc N1-021446**
Budapest, Hungary, 13. – 17. May 2002

Title: Liaison Statement on Deriving IMS parameters from a Pre-Release 5 UICC
Source: CN1
To: CN4
Cc:
Response to:

Contact Person:
Name: Duncan Mills
Tel. Number: +44 1635 676074
E-mail Address: duncan.mills@vf.vodafone.co.uk

Attachments: N1-021461 [CR to 3GPP TS 23.003 v. 5.2.0].

---

1. Overall Description:

As indicated in previous liaison statements copied to CN4, CN1 has been working on a CR to 23.003, specifying the derivation of IMS parameters from the IMSI. Whilst CN1 have the expertise in this particular area, CN4 have ultimate responsibility for agreeing any CRs against 23.003. During the CN1 #24 meeting, CN1 were able to conclude that the attached CR to 23.003 is technically correct. Can CN4 please endorse this decision by formally agreeing the CR?

2. Actions:

To CN4

ACTION: CN1 asks CN4 to agree the attached CR to 23.003

3. Date of Next CN1 Meetings:

CN1_25	29th July – 2nd August 2002	Helsinki, Finland
CN1_26	23rd – 27th September 2002	?, USA

3GPP TSG-CN1 Meeting #24 **Tdoc N1-021455**
Budapest, Hungary, 13. – 17. May 2002

Title: Liaison Statement on 3GPP Network Domain Name usage for IMS
Source: CN1
To: GSMA SerG, GSMA IREG
Cc: CN4, SA2, CN
Response to:

Contact Person:
Name: Sunil Chotai
Tel. Number: +44 1473 605603
E-mail Address: sunil.chotai@o2.com

Attachments: N4-020774[CR to TS 23.003]

---

1. Overall Description:

To help operators in the rollout process of the IMS IP Multimedia capability, R99 and Rel-4 SIM/UICC cards may be used in new Rel-5 mobiles supporting IMS.

It has been identified that a (root) domain is needed by 3GPP for MCC/MNC based address resolution for Rel-5 IMS. ETSI MCC has reserved the domain name **3gppnetwork.org** for 3GPP for this purpose. The GSMA is informed about this domain name. This information will be stored in Rel-5 IMS Mobile Stations (UE) and used if an IMS UE has a R99 or Rel-4 SIM/UICC card.

A UE supporting IMS will send a SIP REGISTER request to the P-CSCF. The P-CSCF needs to be able to route SIP messages to the next hop I-CSCF located in the home network. A DNS lookup is required in the P-CSCF to obtain the IP address of a SIP based I-CSCF server located in the home network associated with the MCC and MNC.

The domain 3gppnetwork.org will be used to enable the DNS look up to obtain the I-CSCF IP address based on the Mobile Country Code (MCC) and Mobile Network Code (MNC) information derived from the IMSI. This information is used by the DNS database queries from P-CSCF.

GSMA needs to consider the roaming impacts on the DNS infrastructure when the mobile is roaming outside the home network and where the P-CSCF is located in the visited network.

The DNS database will need to contain basic addressing information of Mobile Country Codes and Mobile Network Codes and the associated call server (I-CSCF) IP address to support IMS Rel-5. . This is similar to the current GPRS networks where the SGSN performs a DNS lookup to obtain the IP address of the GPRS GGSN node located in the home network associated with the MCC and MNC . It should be noted that this capability defined for IMS may also be reused for other services (for example MMS) that require similar DNS lookups to obtain IP addresses of a (MMS) server located in the network associated with the MCC and MNC.

The attached Change Request to TS 23.003 provides further details on the addressing aspects for IMS.

2. Actions:

To GSMA SerG, GSM A IREG.

ACTION: CN1 request GSMA to note that domain name **IMSI.3gppnetwork.org** has been reserved for 3GPP to support MCC/MNC based address resolution as reflected in TS 23.003 for Release 5. GSMA is kindly asked to progress the relevant practical issues associated in the DNS database management aspects to help in the rollout process of the IMS

3. Date of Next CN1 Meetings:

CN1_25	29th July – 2nd August 2002	Helsinki, Finland
CN1_26	23rd – 27th September 2002	?, USA

3GPP TSG-CN1 Meeting #24 **Tdoc N1-021477**
Budapest, Hungary, 13. – 17. May 2002

Title: **Terminal determination of network support of EDGE**
Source: CN1
To: GERAN, SA1

Contact Person:
Name: **Jeremy Fuller**
Tel. Number: +44 1628 434679
E-mail Address: jfuller@nortelnetworks.com

Attachments: N1-021208

---

1. Overall Description:

Some companies have identified that network support for EDGE is likely to be available prior to full support of Release'99. Concerns were raised that an EDGE enabled terminal may not take advantage of EDGE if it ignores the fact that the network has sent a positive indication of support of EDGE in EDGE specific bits sent on the BCCH, but rather determines the EDGE capabilities of the SGSN based on the presence of the SGSN Revision bit. A more detailed presentation of this topic is provided in the attached document [N1-021208].

It is proposed that a terminal ignores the SGSN revision flag in the context of determining EDGE network capabilities and determines whether the network supports EDGE based on EDGE specific bits sent on the BCCH. When this subject was discussed in CN1 a number of companies supported this approach. However at least one company asked for more time to investigate whether there might be any resulting capability issues in taking this approach

It is hoped that 3GPP can come to a rapid decision on this matter to expedite the successful introduction of EDGE. GERAN and SA1 are asked for their assistance in achieving this.

2. Actions:

To SA1

ACTION: SA1 are asked to identify if they have any concerns with the approach of a terminal determining network support for EDGE based on the EDGE specific parameters it receives, rather than on a parameter indicating support of Release'99. [Note: The network is still mandated to support EDGE in a Release'99 compliant manner]

To GERAN

ACTION: GERAN are asked to review the attached document [N1-021208] and identify any technical concerns in respects to the terminal NOT looking at the SGSN revision bit to determine whether the SGSN supports EDGE. Instead the terminal shall determine support of EDGE based on specific EDGE bits sent on the BCCH.

3. Date of Next CN1 Meetings:

CN1_25	29th July – 2nd August 2002	Helsinki, Finland
CN1_26	23rd – 27th September 2002	?, USA

3GPP TSG-CN1 Meeting #24
Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021389
Revision of N1-021276

CR-Form-v5

CHANGE REQUEST

⌘ **24.008** **CR** **576** ⌘ **rev** **4** ⌘ Current version: **3.11.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Authentication not accepted by MS
Source:	⌘	Siemens
Work item code:	⌘	TEI
Date:	⌘	02.05.2002
Category:	⌘	**F**
Release:	⌘	R99

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	There are two alternative criteria for the MS to reject the network during authentication, MAC failure and invalid SQN. The network is only given two attempts and after that the MS marks the cell as barred. According to 4.7.7.5.1 f) and g), if one of these is met, then the MS shall start a timer to await for a new authentication and then see if the second try was successful. But only the case of two subsequent errors being similar is covered. There is no specification about MAC failure after invalid SQN or vice versa. Note that the sequence 'MAC failure', 'invalid SQN' should not be taken as an indication of a fake network, because it is a possible scenario in a regular network and the 3rd authentication attempt might well be successful.
Summary of change:	⌘	1) Specify that the MS may consider a cell as barred if three faulty authentication challenges are received, never mind which type. 2) If the MS considers a cell as barred, it should abort the RR connection and the PS signalling connection.
Consequences if not approved:	⌘	Security is compromised, because repeated authentication requests become possible.

Clauses affected:	⌘	4.3.2.6.1, 4.7.7.6.1
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ 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/3G_Specs/CRs.htm.
Below is a brief summary:

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

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

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

4.3.2.6.1 MS behaviour towards a network that has failed the authentication procedure

In addition to the cases specified in subclause 4.3.2.6, the MS may deem that the network has failed the authentication check after any combination of three consecutive authentication failures, regardless whether 'MAC failure', 'invalid SQN', or 'GSM authentication unacceptable' was diagnosed. The authentication failures shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3214 or T3216 started after the previous authentication failure is running.

If the MS deems that the network has failed the authentication check, then it should abort the RR connection and the PS signalling connection. Additionally, the MS shall treat the cell where the first failed AUTHENTICATION REQUEST message ~~which lead to sending of AUTHENTICATION FAILURE~~ was received as barred, until refresh of system information data. The MS shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected..

********** NEXT MODIFIED SECTION **********

4.7.7.6.1 MS behaviour towards a network that has failed the authentication procedure

In addition to the cases specified in subclause 4.7.7.6, the MS may deem that the network has failed the authentication check after any combination of three consecutive authentication failures, regardless whether 'MAC failure', 'invalid SQN', or 'GSM authentication unacceptable' was diagnosed. The authentication failures shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3318 or T3320 started after the previous authentication failure is running.

If the MS deems that the network has failed the authentication check, then it should abort the RR connection and the PS signalling connection. Additionally, the MS shall treat the cell where the first failed AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

3GPP TSG-CN1 Meeting #24
Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021390
Revision of N1-021277

CR-Form-v5

CHANGE REQUEST

⌘ **24.008** **CR** **577** ⌘ **rev** **4** ⌘ Current version: **4.6.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Authentication not accepted by MS
Source:	⌘	Siemens
Work item code:	⌘	TEI
Date:	⌘	02.05.2002
Category:	⌘	**A**
Release:	⌘	Rel-4

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	There are two alternative criteria for the MS to reject the network during authentication, MAC failure and invalid SQN. The network is only given two attempts and after that the MS marks the cell as barred. According to 4.7.7.5.1 f) and g), if one of these is met, then the MS shall start a timer to await for a new authentication and then see if the second try was successful. But only the case of two subsequent errors being similar is covered. There is no specification about MAC failure after invalid SQN or vice versa. Note that the sequence 'MAC failure', 'invalid SQN' should not be taken as an indication of a fake network, because it is a possible scenario in a regular network and the 3rd authentication attempt might well be successful.
Summary of change:	⌘	1) Specify that the MS may consider cell barred if three faulty authentication challenges are received, never mind which type. 2) If the MS considers a cell as barred, it should abort the RR connection and the PS signalling connection.
Consequences if not approved:	⌘	Security is compromised, because repeated authentication requests become possible.

Clauses affected:	⌘	4.3.2.6.1, 4.7.7.6.1
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ 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/3G_Specs/CRs.htm.
Below is a brief summary:

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

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

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

4.3.2.6.1 MS behaviour towards a network that has failed the authentication procedure

In addition to the cases specified in subclause 4.3.2.6, the MS may deem that the network has failed the authentication check after any combination of three consecutive authentication failures, regardless whether 'MAC failure', 'invalid SQN', or 'GSM authentication unacceptable' was diagnosed. The authentication failures shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3214 or T3216 started after the previous authentication failure is running.

If the MS deems that the network has failed the authentication check, then ~~the~~ it should abort the RR connection and the PS signalling connection. Additionally, the MS shall treat the cell where the first failed AUTHENTICATION REQUEST message ~~which lead to sending of AUTHENTICATION FAILURE~~ was received as barred, until refresh of system information data. The MS shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

********** NEXT MODIFIED SECTION **********

4.7.7.6.1 MS behaviour towards a network that has failed the authentication procedure

In addition to the cases specified in subclause 4.7.7.6, the MS may deem that the network has failed the authentication check after any combination of three consecutive authentication failures, regardless whether 'MAC failure', 'invalid SQN', or 'GSM authentication unacceptable' was diagnosed. The authentication failures shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3318 or T3320 started after the previous authentication failure is running.

If the MS deems that the network has failed the authentication check, then it should abort the RR connection and the PS signalling connection. Additionally, the MS shall treat the cell where the first failed AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

3GPP TSG-CN1 Meeting #24
Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021278
Revision of N1-020880

CR-Form-v5

CHANGE REQUEST

⌘ **24.008** **CR** **578** ⌘ **rev** **2** ⌘ Current version: **5.3.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Authentication not accepted by MS
Source:	⌘	Siemens
Work item code:	⌘	TEI
Date:	⌘	11.4.2002
Category:	⌘	**A**
Release:	⌘	Rel-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘

1) There are two alternative criteria for the MS to reject the network during authentication, MAC failure and invalid SQN. The network is only given two attempts and after that the MS marks the cell as barred.

According to 4.7.7.5.1 f) and g), if one of these is met, then the MS shall start a timer to await for a new authentication and then see if the second try was successful. But only the case of two subsequent errors being similar is covered. There is no specification about MAC failure after invalid SQN or vice versa.

Note that the sequence 'MAC failure', 'invalid SQN' should not be taken as an indication of a fake network, because it is a possible scenario in a regular network and the 3rd authentication attempt might well be successful.

2) In 4.3.2.6 c) and 4.7.7.6 f), the retransmission timers need to be stopped also if the MS detects an unacceptable GSM authentication.

3) In 4.7.7.6 f) and g), the error type "GSM authentication unacceptable" can occur also as a result of the second AUTHENTICATION & CIPHERING REQUEST.

Summary of change: ⌘

- Specify that the MS shall consider cell barred if three faulty authentication challenges are received, never mind which type.
- The condition that the MS shall consider the cell as barred, if two authentication errors of the same type were diagnosed, is removed.
- Clarify that the new AUTHENTICATION & CIPHERING REQUEST has to contain a UMTS authentication challenge, when it is sent to an MS supporting UMTS authentication roaming in a UMTS cell.
- Clarify that the MS aborts the RR connection, if the network fails the authentication.

Consequences if not approved: ⌘

Security is compromised because repeated authentication requests become possible.

Clauses affected:	⌘	4.3.2.6, 4.3.2.6.1, 4.7.7.6, 4.7.7.6.1		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ 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/3G_Specs/CRs.htm. Below is a brief summary:

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

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

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

4.3.2.6 Abnormal cases

(a) RR connection failure:

Upon detection of a RR connection failure before the AUTHENTICATION RESPONSE is received, the network shall release all MM connections (if any) and abort any ongoing MM specific procedure.

(b) Expiry of timer T3260:

The authentication procedure is supervised on the network side by the timer T3260. At expiry of this timer the network may release the RR connection. In this case the network shall abort the authentication procedure and any ongoing MM specific procedure, release all MM connections if any, and initiate the RR connection release procedure described in subclause 3.5.

(c) Authentication failure (reject cause "MAC failure" or "GSM authentication unacceptable"):

The MS shall send an AUTHENTICATION FAILURE message, with reject cause "MAC failure" or "GSM authentication unacceptable" according to subclause 4.3.2.5.1, to the network and start timer T3214. Furthermore, the MS shall stop any of the retransmission timers that are running (e.g. T3210, T3220 or T3230). Upon the first receipt of an AUTHENTICATION FAILURE message from the MS~~,~~ with reject cause "MAC failure" or "GSM authentication unacceptable", the network may initiate the identification procedure described in subclause 4.3.3. This is to allow the network to obtain the IMSI from the MS. The network may then check that the TMSI originally used in the authentication challenge corresponded to the correct IMSI. Upon receipt of the IDENTITY REQUEST message from the network, the MS shall send the IDENTITY RESPONSE message.

NOTE: Upon receipt of an AUTHENTICATION FAILURE message from the MS with reject cause "MAC failure" or "GSM authentication unacceptable", the network may also terminate the authentication procedure (see subclause 4.3.2.5).

If the TMSI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION REQUEST message to the MS. Upon receiving the new~~second~~ AUTHENTICATION REQUEST message from the network, the MS shall stop the timer T3214, if running, and then process the challenge information as normal.

~~When the first AUTHENTICATION REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (i.e. T3210, T3220 or T3230).~~

~~Upon successfully validating~~ If the network is validated successfully (an AUTHENTICATION REQUEST that contains a valid SQN and MAC is received), the MS shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first failed AUTHENTICATION REQUEST message ~~containing an invalid MAC~~.

If the MS receives the second AUTHENTICATION REQUEST while T3214 is running, and the MAC value cannot be resolved or the message contains a GSM authentication challenge, the MS shall follow the procedure specified in this subclause (c), starting again fom the beginning. If the SQN is invalid, the MS shall proceed as specified in (d).

It can be assumed that the source of the authentication challenge is not genuine (authentication not accepted by the MS) if any of the following occur:

- ~~A~~after sending the AUTHENTICATION FAILURE message with the reject cause "MAC failure" or "GSM authentication unacceptable" the timer T3214 expires~~.~~;

- the MS detects any combination of the authentication failures: "MAC failure", "invalid SQN", and "GSM authentication unacceptable", during three consecutive authentication challenges. The authentication challenges shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3214 or T3216 started after the previous authentication failure is running.

~~- Upon receipt of the second AUTHENTICATION REQUEST while T3214 is running and the MAC value cannot be resolved.~~

~~The second AUTHENTICATION REQUEST which is received while T3214 is running is GSM authentication challenge (i.e. no AUTN parameter was received).~~

When it has been deemed by the MS that the source of the authentication challenge is not genuine (i.e. authentication not accepted by the MS), the MS shall behave as described in subclause 4.3.2.6.1.

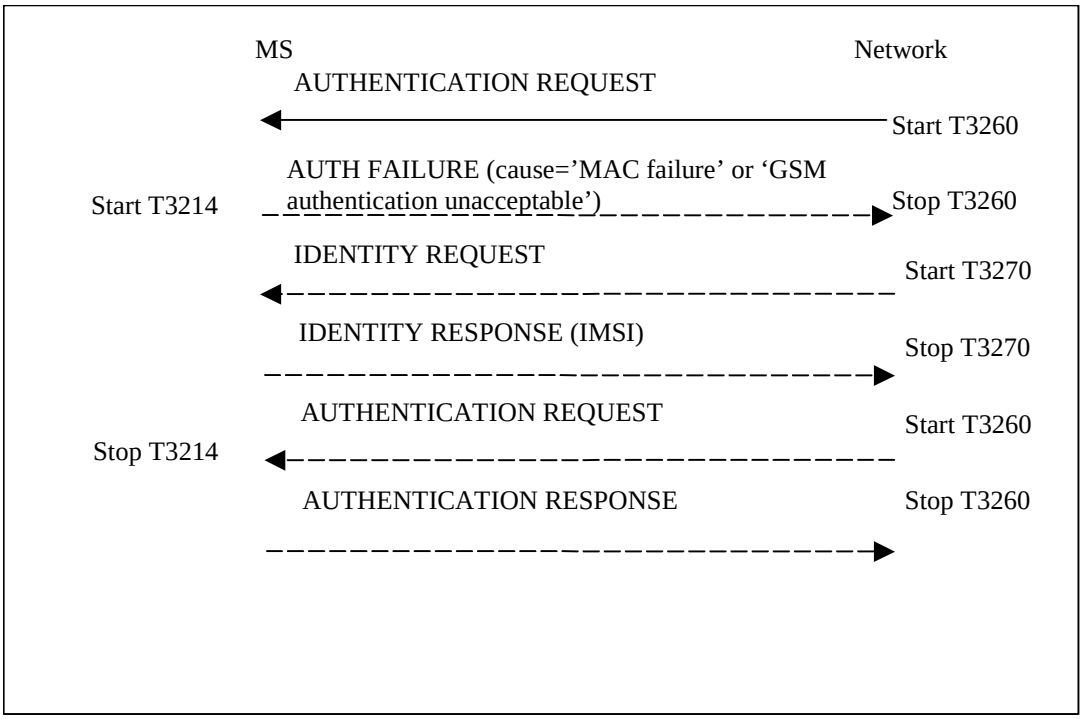


Figure 4.2/3GPP TS 24.008: Authentication Failure Procedure (reject cause "MAC failure" or "GSM authentication unacceptable")

(d) Authentication failure (reject cause "synch failure"):

The MS shall send an AUTHENTICATION FAILURE message, with reject cause "synch failure", to the network and start the timer T3216. Furthermore, the MS shall stop any of the retransmission timers that are running (e.g. T3210, T3220 or T3230). Upon the first receipt of an AUTHENTICATION FAILURE message from the MS with the reject cause "synch failure", the network shall use the returned AUTS parameter from the authentication failure parameter IE in the AUTHENTICATION FAILURE message, to re-synchronise. The re-synchronisation procedure requires the VLR/MSC to delete all unused authentication vectors for that IMSI and obtain new vectors from the HLR. When re-synchronisation is complete, the network shall initiate the authentication procedure. Upon receipt of the AUTHENTICATION REQUEST message, the MS shall stop the timer T3216, if running.

NOTE: Upon receipt of two consecutive AUTHENTICATION FAILURE messages from the MS with reject cause "synch failure", the network may terminate the authentication procedure by sending an AUTHENTICATION REJECT message.

~~When the first AUTHENTICATION REQUEST message containing an invalid SQN has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (i.e. T3210, T3220 or T3230).~~

~~Upon successfully validating~~ If the network is validated successfully (a new~~second~~ AUTHENTICATION REQUEST is received which contains a valid SQN and MAC) while T3216 is running, the MS shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first failed AUTHENTICATION REQUEST message ~~containing an invalid SQN~~.

If the MS receives the second AUTHENTICATION REQUEST while T3216 is running, and the MAC value cannot be resolved or the message contains a GSM authentication challenge, the MS shall proceed as specified in

(c); if the SQN is invalid, the MS shall follow the procedure specified in this subclause (d), starting again fom the beginning.

The MS shall deem that the network has failed the authentication check and behave as described in subclause 4.3.2.6.1, if any of the following occurs:

~~If the MS receives a second AUTHENTICATION REQUEST which contains an invalid SQN or GSM AUTHENTICATION REQUEST while T3216 is running, then the MS shall behave as described in subclause 4.3.2.6.1.~~

- ~~If~~ the timer T3216 expires~~, then the MS shall behave as described in subclause 4.3.2.6.1.~~;

- the MS detects any combination of the authentication failures: "MAC failure", "invalid SQN", and "GSM authentication unacceptable", during three consecutive authentication challenges. The authentication challenges shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3214 or T3216 started after the previous authentication failure is running.

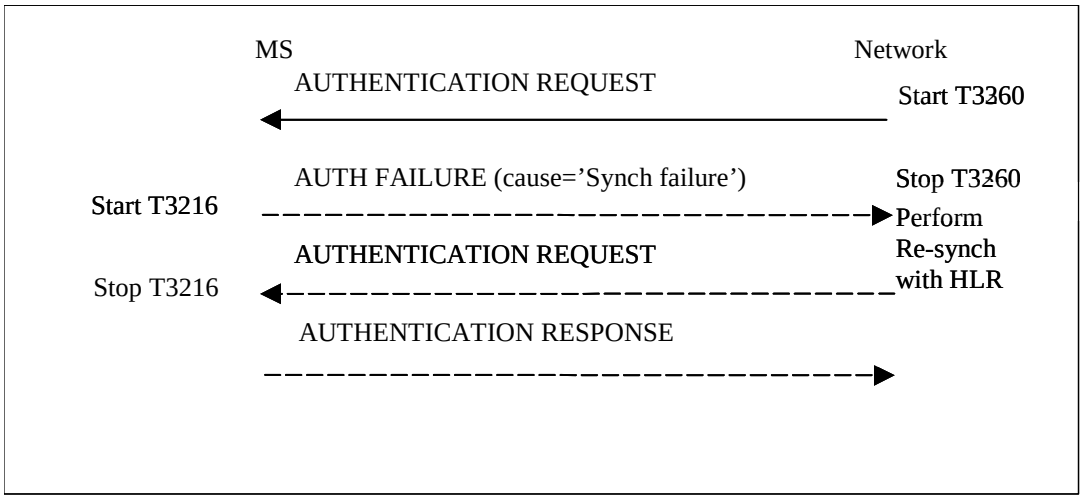


Figure 4.2a/3GPP TS 24.008: Authentication Failure Procedure (reject cause "Synch failure")

4.3.2.6.1 MS behaviour towards a network that has failed the authentication procedure

If the MS deems that the network has failed the authentication check, then ~~the~~ it shall abort the RR connection and the PS signalling connection and treat the cell where the first failed AUTHENTICATION REQUEST message ~~which lead to sending of AUTHENTICATION FAILURE~~ was received as barred, until refresh of system information data. The MS shall start any retransmission timers (e.g. T3210, T3220 or T3230), if they were running and stopped when the MS received the first AUTHENTICATION REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

********** NEXT MODIFIED SECTION **********

4.7.7.6 Abnormal cases ~~on the network side~~

The following abnormal cases can be identified:

a) Lower layer failure

Upon detection of a lower layer failure before the AUTHENTICATION AND CIPHERING RESPONSE is received, the network shall abort the procedure.

b) Expiry of timer T3360

The network shall, on the first expiry of the timer T3360, retransmit the AUTHENTICATION AND CIPHERING REQUEST and shall reset and start timer T3360. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3360, the procedure shall be aborted.

c) Collision of an authentication and ciphering procedure with a GPRS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing authentication procedure has been completed and no GPRS attach procedure is pending on the network (i.e. no ATTACH ACCEPT/REJECT message has to be sent as an answer to an ATTACH REQUEST message), the network shall abort the authentication and ciphering procedure and proceed with the new GPRS attach procedure.

d) Collision of an authentication and ciphering procedure with a GPRS attach procedure when the authentication and ciphering procedure has been caused by a previous GPRS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing authentication procedure has been completed and a GPRS attach procedure is pending (i.e. an ATTACH ACCEPT/REJECT message has still to be sent as an answer to an earlier ATTACH REQUEST message), then:

- If one or more of the information elements in the ATTACH REQUEST message differs from the ones received within the previous ATTACH REQUEST message, the network shall not treat the authentication any further and proceed with the GPRS attach procedure; or
- If the information elements do not differ, then the network shall not treat any further this new ATTACH REQUEST.

Collision of an authentication and ciphering procedure with a GPRS detach procedure

GPRS detach containing cause "power off":

If the network receives a DETACH REQUEST message before the ongoing authentication and ciphering procedure has been completed, the network shall abort the authentication and ciphering procedure and shall progress the GPRS detach procedure.

GPRS detach containing other causes than "power off":

If the network receives a DETACH REQUEST message before the ongoing authentication and ciphering procedure has been completed, the network shall complete the authentication and ciphering procedure and shall respond to the GPRS detach procedure as described in subclause 4.7.4.

e) Collision of an authentication and ciphering procedure with a routing area updating procedure

If the network receives a ROUTING AREA UPDATE REQUEST message before the ongoing authentication procedure has been completed, the network shall progress both procedures.

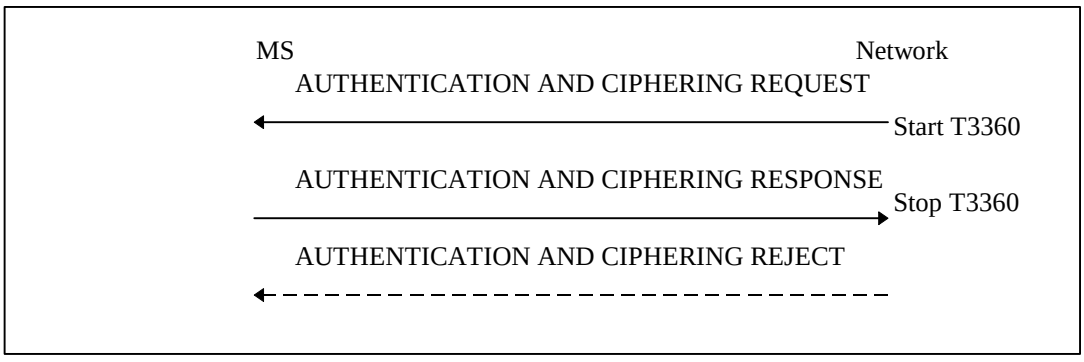


Figure 4.7.7/1 3GPP TS 24.008: Authentication and ciphering procedure

(f) Authentication failure (GMM cause "MAC failure" or "GSM authentication unacceptable")

The MS shall send an AUTHENTICATION & CIPHERING FAILURE message, with GMM cause ‘MAC failure’ or ‘GSM authentication unacceptable’ according to subclause 4.7.7.5.1, to the network and start timer T3318. Furthermore, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317). Upon the first receipt of an AUTHENTICATION & CIPHERING FAILURE message from

the MS with GMM cause ‘MAC failure’ or ‘GSM authentication unacceptable’ the network may initiate the identification procedure described in subclause 4.7.8. This is to allow the network to obtain the IMSI from the MS. The network may then check that the P-TMSI originally used in the authentication challenge corresponded to the correct IMSI. Upon receipt of the IDENTITY REQUEST message from the network, the MS shall send the IDENTITY RESPONSE message.

NOTE: Upon receipt of an AUTHENTICATION & CIPHERING FAILURE message from the MS with reject cause "MAC failure" or "GSM authentication unacceptable", the network may also terminate the authentication procedure (see subclause 4.7.7.5).

If the P-TMSI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION & CIPHERING REQUEST message to the MS. Upon receiving the newsecond AUTHENTICATION & CIPHERING REQUEST message from the network, the MS shall stop timer T3318, if running, and then process the challenge information as normal.

When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid MAC has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317).

Upon successfully validating If the network, is validated successfully (an AUTHENTICATION & CIPHERING REQUEST message that contains a valid SQN and MAC is received), the MS shall send the AUTHENTICATION & CIPHERING RESPONSE message to the network and shall start any retransmission timers (i.e.g. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first failed AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC.

If the MS receives the second AUTHENTICATION AND CIPHERING REQUEST while T3318 is running and

- the MAC value cannot be resolved; or

- the message was received in UMTS and contains a GSM authentication challenge,

the MS shall follow the procedure specified in this subclause (f), starting again fom the beginning. If the SQN is invalid, the MS shall proceed as specified in (g).

It can be assumed that the source of the authentication challenge is not genuine (authentication not accepted by the MS) if any of the following occurs:

- Aafter sending the AUTHENTICATION & CIPHERING FAILURE message with GMM cause ‘MAC failure’ or ‘GSM authentication unacceptable’ the timer T3318 expires;

- Upon receipt of the second AUTHENTICATION & CIPHERING REQUEST message from the network while the T3318 is running and the MAC value cannot be resolved;

- The second AUTHENTICATION REQUEST & CIPHERING REQUEST which is received in UMTS while T3318 is running is a GSM authentication challenge (i.e. no AUTN parameter was received).

- the MS detects any combination of the authentication failures: "MAC failure", "invalid SQN", and "GSM authentication unacceptable", during three consecutive authentication challenges. The authentication challenges shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3318 or T3320 started after the previous authentication failure is running.

When it has been deemed by the MS that the source of the authentication challenge is not genuine (authentication not accepted by the MS), the MS shall behave as described in subclause 4.7.7.6.1.

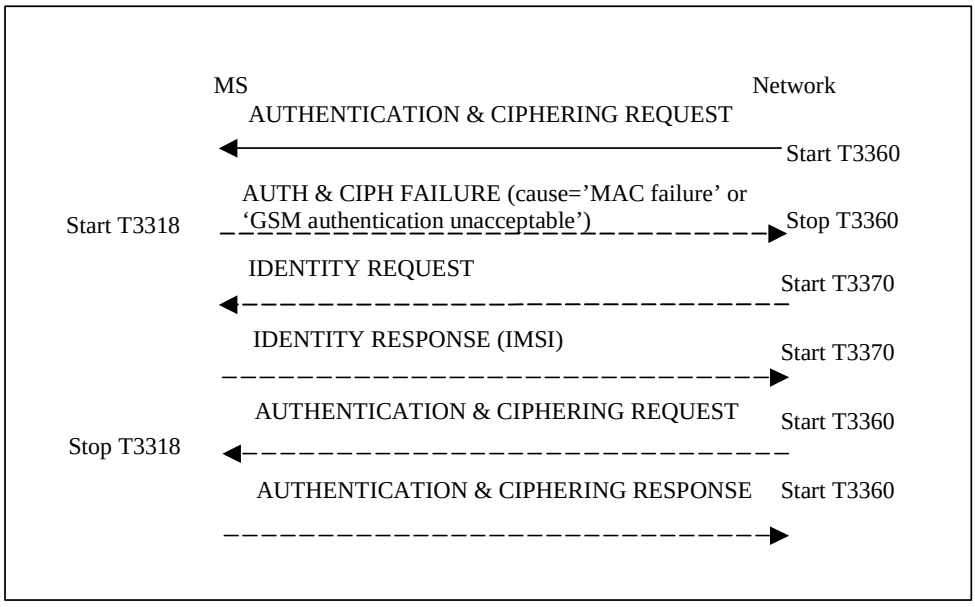


Figure 4.7.7a/1 3GPP TS 24.008: Authentication failure cause "MAC failure" or "GSM authentication unacceptable"

(g) Authentication failure (GMM cause "Synch failure"):

The MS shall send an AUTHENTICATION & CIPHERING FAILURE message, with the GMM cause "Synch failure", to the network and start the timer T3320. Furthermore, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317). Upon the first receipt of an AUTHENTICATION & CIPHERING message from the MS with the GMM cause "synch failure", the network shall use the returned AUTS parameter from the authentication & ciphering failure parameter IE in the AUTHENTICATION & CIPHERING FAILURE message, to re-synchronise. The re-synchronisation procedure requires the SGSN to delete all unused authentication vectors for that IMSI and obtain new vectors from the HLR. When re-synchronisation is complete, the network shall initiate the authentication & ciphering procedure. Upon receipt of the AUTHENTICATION & CIPHERING REQUEST message, the MS shall stop timer T3320, if running.

NOTE: Upon receipt of two consecutive AUTHENTICATION & CIPHERING FAILURE messages from the MS with reject cause "synch failure", the network may terminate the authentication procedure by sending an AUTHENTICATION & CIPHERING REJECT message.

~~When the first AUTHENTICATION & CIPHERING REQUEST message containing an invalid SQN has been received by the MS from the network, the MS shall stop any of the retransmission timers that are running (e.g. T3310, T3321, T3330 or T3317).~~

~~Upon successfully validating~~ If the network, is validated successfully (a new~~second~~ AUTHENTICATION & CIPHERING REQUEST message is received which contains a valid SQN and MAC) while T3320 is running, the MS shall send the AUTHENTICATION & CIPHERING RESPONSE message to the network and shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first failed AUTHENTICATION AND CIPHERING REQUEST message ~~containing an invalid SQN~~.

If the MS receives the second AUTHENTICATION & CIPHERING REQUEST while T3320 is running and

- the MAC value cannot be resolved; or

- the message was received in UMTS and contains a GSM authentication challenge,

the MS shall proceed as specified in (f). If the SQN is invalid, the MS shall follow the procedure specified in this subclause (g), starting again fom the beginning.

The MS shall deem that the network has failed the authentication check and behave as described in subclause 4.7.7.6.1, if any of the following occurs:

~~If the MS receives a second AUTHENTICATION & CIPHERING REQUEST message which contains an invalid SQN while T3320 is running, then the MS shall behave as described in subclause 4.7.7.6.1.~~

- ~~If~~ the timer T3320 expires~~;, the MS shall behave as described in subclause 4.7.7.6.1.~~

- the MS detects any combination of the authentication failures: "MAC failure", "invalid SQN", and "GSM authentication unacceptable", during three consecutive authentication challenges. The authentication challenges shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the MS, while the timer T3318 or T3320 started after the previous authentication failure is running.

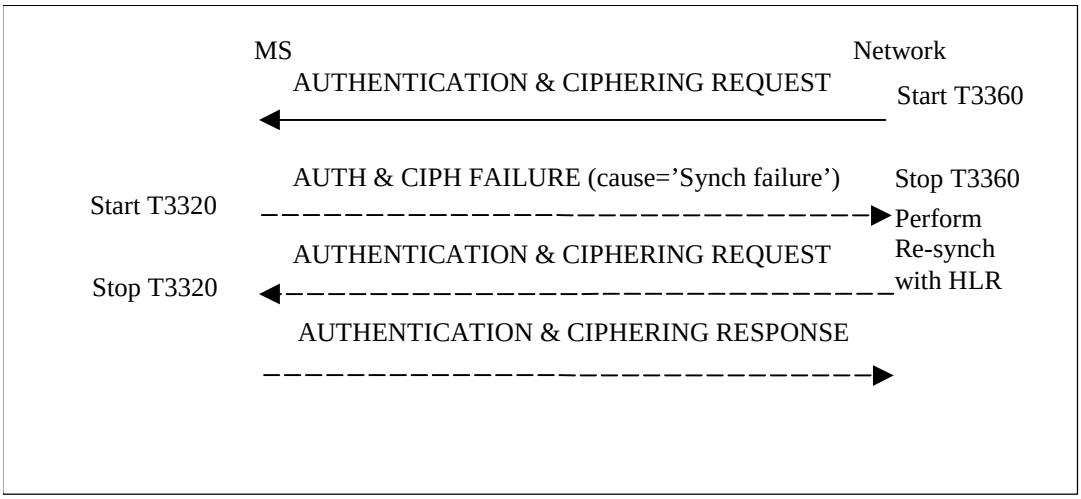


Figure 4.7.7b/1 3GPP TS 24.008: Authentication failure cause 'Synch failure'

4.7.7.6.1 MS behaviour towards a network that has failed the authentication procedure

If the MS deems that the network has failed the authentication check, then it shall abort the RR connection and the PS signalling connection and treat the cell where the first failed AUTHENTICATION & CIPHERING REQUEST message was received as barred, until refresh of system information data. The MS shall start any retransmission timers (i.e. T3310, T3321, T3330 or T3317), if they were running and stopped when the MS received the first AUTHENTICATION AND CIPHERING REQUEST message containing an invalid MAC or invalid SQN, or no AUTN when a UMTS authentication challenge was expected.

3GPP TSG CN WG4 Meeting #14 ***N4-020774***
Budapest, Hungary, 13th – 17th May 2002 **revision of N1-021445 (N4-020757)**

3GPP TSG-CN1 Meeting #24 ***Tdoc N1-021461***
Budapest, Hungary, 13. – 17. May 2002 **revision of N1-021445 (N1-021329)**

CR-Form-v5

CHANGE REQUEST

⌘ **23.003** **CR** **041** ⌘ **rev** **2** ⌘ Current version: **5.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Use of a temporary public user identity
Source:	⌘	Vodafone, Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	1st May 2002
Category:	⌘	**F**
Release:	⌘	REL-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	SA2 have agreed the stage two for IMS access with a R99/Rel-4 USIM. In order to align with the stage two, it is now necessary to add the procedures to derive domain name, private user identity and public user identity from the IMSI.
Summary of change:	⌘	Addition of conversion procedures in a new section on IMS.
Consequences if not approved:	⌘	Pre-Release-5 USIMs not supported by IMS

Clauses affected:	⌘	
Other specs affected:	⌘	☐ Other core specifications ⌘
		☐ Test specifications
		☐ 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/3G_Specs/CRs.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.

1.1 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 TS 21.905: "3G Vocabulary".

[2] 3GPP TS 23.008: "Organization of subscriber data".

[3] Void.

[4] 3GPP TS 23.070: "Routeing of calls to/from Public Data Networks (PDN)".

[5] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[6] 3GPP TS 29.060: "GPRS Tunnelling protocol (GPT) across the Gn and Gp interface".

[7] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[8] GSM 09.03: "Digital cellular telecommunications system (Phase 2+); Signalling requirements on interworking between the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) and the Public Land Mobile Network (PLMN)".

[9] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

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

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

[12] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land Mobile Stations in public land mobile networks (PLMN)".

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

[14] RFC 791: "Internet Protocol".

[15] RFC 1883: "Internet Protocol, Version 6 (IPv6) Specification".

[16] 3GPP TS 25.401: "UTRAN Overall Description".

[17] 3GPP TS 25.413: "UTRAN Iu Interface RANAP Signalling".

[18] RFC 2181: “Clarifications to the DNS Specification”.

[19] RFC 1035: “Domain Names - Implementation and Specification”.

[20] RFC 1123: “Requirements for Internet Hosts -- Application and Support”.

[21] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes".

[22] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2"

[23] RFC 2486: "The Network Access Identifier"

[24] RFC 3261: "SIP: Session Initiation Protocol"

[25] 3GPP TS 31.102: "Characteristics of the USIM Application."

[26] RFC 1035: "Domain names – implementation and specification"

*** Proposed New Section ***

13 Numbering, addressing and identification within the IP multimedia core network subsystem

13.1 Introduction

This clause describes the format of the parameters needed to access the IP multimedia core network subsystem. For further information on the use of the parameters see 3GPP TS 23.228 [22].

13.2 Home network domain name

The home network domain name shall be in the form of an Internet domain name, e.g. operator.com, as specified in RFC 1035 [26].

If there is no ISIM application, the UE shall derive the home network domain name from the IMSI as described in the following steps:

~~1. remove any non-decimal digits from the IMSI, leaving a string of 15 or less digits;~~

~~2~~1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [25]) and separate them into MCC and MNC with "."; and

~~3~~2. reverse the order of the MCC and MNC. Append to the result: ".IMSI.3gppnetwork.org"

An example of a home network domain name is:

EXAMPLE: IMSI in use: 234150999999999;

where;

MCC: 234;

MNC: 15;

MSIN: 0999999999; and

home domain name: 15.234.IMSI.3gppnetwork.org.

13.3 Private user identity

The private user identity shall take the form of an NAI, and shall have the form user@realm as specified in clause 3 of RFC2486 [23].

NOTE: It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

If there is no ISIM application, the private user identity is not known. In this case, the private user identity is derived from the IMSI.

The following steps show how to build the private user identity out of the IMSI:

~~1. remove any non-decimal digits from the IMSI, leaving a string of 15 or less digits;~~

1~~2~~. use ~~the result from step 1, i.e.~~ the whole string of digits~~,~~ as the user part of the private user identity; and

2~~3~~. the first digits of the IMSI, i.e. MNC and MCC, will be converted into a domain name, as described in subclause 13.2~~1~~.

The result will be a private user identity of the form imsi@mnc.mcc."IMSI.3gppnetwork.org". For example: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the private user identity then takes the form 234150999999999@15.234.IMSI.3gppnetwork.org

13.4 Public user identity

The public user identity shall take the form of either a SIP URI, see RFC3261[24] or an E.164 number. A SIP URI shall take the form "sip:user@domain".

~~In case~~If there is no ISIM application to host the public user identity, a temporary public user identity shall be derived, based on the IMSI. The temporary public user identity shall be of the form "user@domain" and shall therefore be equal to the private user identity. The private user identity is derived as per subclause 13.2. That is, the private user identity will be appended to the string "sip:"

EXAMPLE: "sip:234150999999999@15.234.IMSI.3gppnetwork.org".

3GPP TSG-CN1 Meeting #24 ***Tdoc N1-021405***

Budapest, Hungary, 13. – 17. May 2002 ~~***Tdoc N1-021317, N1-021122, N1-021250***~~

CR-Form-v5

CHANGE REQUEST

⌘ **TS 23.218 CR 003** ⌘ **rev 10** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Clarification on SPI related text
Source:	⌘	dynamicsoft, Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	2002/05/13
Category:	⌘	**F**
Release:	⌘	REL-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change: ⌘
1) In the current text, default handling procedure is initiated when AS is failed. However, there is no description about the treatment of remaining filter criteria list.
2) Clarify that the S-CSCF downloads and stores the filter criteria (profile subset) from the HSS.
3) Clarify precedence in handling of "barring" versus triggers
4) Delete reference to "refreshing dialogue".

Summary of change: ⌘ **Previous T-doc no at CN1#23: N1-020953; then #23 SIP Ad Hoc 021102**
1) In section 5.2, it is proposed to describe that the default handling procedure will abandon the remaining filter criteria list
2) Confirm that triggers apply solely to dialogue initiation

Consequences if not approved: ⌘
1) Default handling procedure will be implemented wrongly.
2) Possible confusion that triggers apply not only to dialogue initiation

Clauses affected: ⌘ 5.2, 6.4, 6.5, 6.9, 7.2.1, B.3.1

Other specs affected: ⌘
☐ Other core specifications ⌘
☐ Test specifications
☐ O&M Specifications

Other comments: ⌘ Changes done on this CR version:
1) note2 (5.2)
2) barring verification, iFC download, minor edit 1st para. (6.4)
3) deletion of refreshing (6.4, 6.5.1, 6.5.2)
4) verification of barred user (6.5.1, 6.5.2)

	5) reference to XML (6.9.2) 6) Default handling & AS being FFS (6.9.2.2)

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.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.

Change

5.2 Service interaction with IP multimedia subsystem

Service Points of Interest (SPIs) are those points in the SIP signalling on which Filter Criteria can be set. The following SPIs are defined:

- any initial known or unknown SIP method (e.g. REGISTER, INVITE, SUBSCRIBE, MESSAGE);
- presence or absence of any header;
- content of any header;
- direction of the request is with respect to the served user – either mobile originated (MO) or mobile terminated (MT) or mobile terminated to unregistered user;

  NOTE 1: REGISTER is considered part of the Mobile Origination.

  NOTE 2: The S-CSCF shall verify if the end user is barred before checking if any trigger applies for that end user.

- session description information.

A Filter Criteria triggers one or more SPIs in order to send the related request to one specific application server. The set of Filter Criteria that is stored for a service profile of a specific user is called "Application Server Subscription Information". In order to allow the S-CSCF to handle the different Filter Criteria in the right sequence, a priority shall be assigned to each of them. ~~Additionally Filter Criteria may indicate that a dialog shall be released and abandon the servicing of the remaining list of filter criteria be terminated if the indicated Application Server cannot be reached or the AS requests to perform the default handling procedure.~~ If the S-CSCF can not reach the AS, the S-CSCF shall apply the default handling associated with the trigger. This default handling shall be :

- To continue verifying ~~of~~ if the triggers of lower priority in the list match; or
- To abandon verification of matching of the triggers of lower priority in the list; and to release the dialogue.

Therefore a Filter Criteria shall contain the following information:

- address of the Application Server to be contacted;
- priority of the Filter Criteria providing the sequence in which the criteria shall be applied;
- trigger Points, which indicated the Service Points of Interest (SPIs) triggered by this Filter Criteria. The SPIs may be linked by means of logical expressions (AND, OR, NOT, etc.);
- default ~~H~~handling (as described above). ~~, i.e. indication if the dialog shall be released and abandon the servicing of the remaining list of filter criteria be terminated if the AS cannot be reached or the AS requests to perform the default handling procedure.;~~
- optional Service Information that shall be added to the message body before it is sent to the AS (as an example this may include the IMSI for the IM-SSF).

The same priority shall not be assigned to more than one initial Filter Criteria~~to more than one AS~~) for a given end user.

In the case that multiple Filter Criteria are sent from the HSS to the S-CSCF when the S-CSCF receives a message via the Mw interface, the S-CSCF shall check the filter criteria one by one according to their indicated priority, i.e. the S-CSCF shall:

1. set up the list of filter criteria for that request according to their priority – the sequence of the filter criteria shall not be changed until the request finally leaves the S-CSCF via the Mw interface again;
2. parse the received request in order to find out the Service Points of Interest (SPIs) that are included in it;
3. check whether the trigger points of the filter criteria with the next highest priority are matched by the SPIs of the request and

a) if it does not match the S-CSCF shall immediately proceed with step ~~6~~ 4;

b) if it matches the S-CSCF shall:

i) add an indication to the request which will allow the S-CSCF to identify the message on the incoming side, even if its dialog identification has been changed e.g. due to the AS performing third party call control;

ii) forward the request via the ISC interface to the AS indicated in the current filter criteria. The AS then performs the service logic, may modify the request and may send the request back to the S-CSCF via the ISC interface;

iii) proceed with step ~~6~~ 4 if the request was received again from the AS via the ISC interface;

4~~6~~. repeat the above steps 2 ~~to 5~~ and 3 for every filter criteria which was initially set up (in step 1) until the last filter criteria has been checked;

5~~7~~. route the request based on normal SIP routing behaviour.

If an Application Server decides to locally terminate a request and ~~and~~ , sends back a final response for that request ~~and reqests a default handling procedure~~ via the ISC interface to the S-CSCF, the S-CSCF shall abandon verification of the matching of the triggers of lower priority in the list~~perform the default handling treatment , i.e. discard the remaining list of filter criteria for that request~~. The final response shall include the indicator defined in step 3 b) i) above, so that the S-CSCF can correlate the messages.

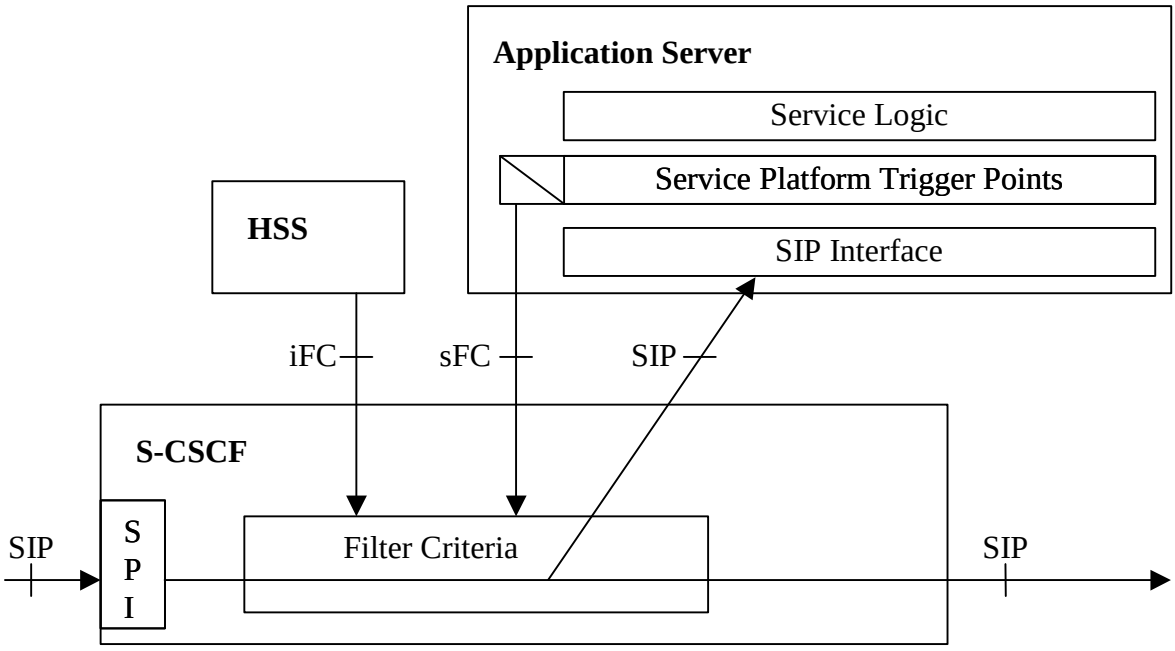


Figure 5.2.1: Application triggering architecture

Each invoked Application Server/service logic may decide not to be engaged with the invoked session by indicating that during the very first SIP transaction when the Record-Route/Route is generated for subsequent SIP requests. The denial shall mean that subsequent requests shall not be routed to such Application Servers/service logic any more during the lifetime of that session. Any Application Server, which has determined that it will not receive subsequent requests for a session cannot revoke this determination by means of Initial Filter Criteria (iFC).

Change

6.4 Handling of mobile originated IP multimedia sessions

The S-CSCF shall verify if the public user identity is barred. If so, it shall respond with a 4xx error code and stop further session processing.

The S-CSCF only looks for initial filter criteria when receiving an initial request ~~or refreshing request for a dialog...~~

The initial filter criteria (subset of the profile) has already been downloaded from the HSS and is stored locally at the S-CSCF, as specified in 3GPP TS 24.228 [4], and 3GPP TS 24.229 [5].

When such a session request comes in, the S-CSCF shall first check its triggers points (i.e., this is ~~an~~ a mobile originating request or a mobile terminating request). This clause describes the requirements for the S-CSCF when this request is ~~an~~ a mobile originating request. So ~~, if this request is an originating request,~~ the S-CSCF shall:

- check whether this request matches the initial filter criteria with the highest priority ~~of the application servers assigned~~ for that user by checking the service profile against the public user identity, which was used to place this request;

  if this request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server;

- if this request does not match the highest priority initial filter criteria, check for matching of the following filter criteria priorities until one applies;

- if no more (or none) of the initial filter criteria apply, ~~of any application server,~~ the S-CSCF shall forward this request downstream based on the route decision;

- ~~if this request matches the initial filter criteria of only one application server and the S-CSCF has not interacted with that application server during this initial or refreshing transaction, the S-CSCF shall forward this request to that application server; if the S-CSCF has interacted with that application server in this transaction, the S-CSCF shall not forward this request to that application server but shall forward this request downstream based on the route decision;~~

- ~~if this originating request matches the initial filter criteria of more than one application server, the S-CSCF shall forward this request to the one which has not been interacted with in this transaction and has the highest priority according the Priority List given by HSS among those matched application servers; if all of them have been interacted in this transaction, the S-CSCF shall forward this request downstream based on the route decision; if the first attempt fails, the S-CSCF shall try others one by one according to their priories until there is a successful contact;~~

- in any instance, if the contact of the application server fails, the S-CSCF shall use the "default handling ~~treatment~~" associated with the ~~SPI~~initial Filter Criteria to determine if it shall either terminate the call, or let the call continue based on the information in the filter criteria; if the filter criteria doesn't contain instruction to the S-CSCF regarding the failure of the contact to the application server, the S-CSCF shall let the call continue as the default behaviour.

6.5 Handling of mobile terminated IP multimedia sessions

6.5.1 Handling of mobile terminated IP multimedia sessions, registered user

The S-CSCF shall verify if the public user identity is barred. If so, it shall respond with a 4xx error code and stop further session processing.

The S-CSCF only looks for initial filter criteria when receiving an initial request ~~or refreshing request for a dialog~~.

When such a request comes in, the S-CSCF shall first check this is an originating request or a terminating request. This clause describes the requirements for the S-CSCF when this request is a terminating request. So, if this request is a terminating request, the S-CSCF shall:

- if unavailable, download the relevant subscriber profile including the initial filter criteria from the HSS.
- use the initial Filter Criteria for the Mobile Termination;
  - ~~check whether this request matches the initial filter criteria of the application servers assigned for that user by checking the service profile against the public user identity, which this request was addressed to;~~
- the subsequent requirements for the S-CSCF are the same as those for handling originating sessions.

It may be possible that originating UE and terminating UE shares the same S-CSCF and AS, therefore the shared application server may interact with the S-CSCF twice in one transaction but in originating and terminating procedures respectively.

6.5.2 Handling of mobile terminated IP multimedia sessions, unregistered user

The S-CSCF shall verify if the public user identity is barred. If so, it shall respond with a 4xx error code and stop further session processing.

The S-CSCF only looks for initial filter criteria when receiving an initial request.

When such a request comes in, the S-CSCF shall first check this is an originating request or a terminating request. This clause describes the requirements for the S-CSCF when this request is a terminating request. So, if this request is a terminating request, the S-CSCF shall:

- if unavailable, download the relevant subscriber profile including the initial filter criteria from the HSS.
- use the initial Filter Criteria for the Mobile Termination for unregistered user;
- the subsequent requirements for the S-CSCF are the same as those for handling originating sessions.

It may be possible that originating UE and terminating UE shares the same S-CSCF and AS, therefore the shared application server may interact with the S-CSCF twice in one transaction but in originating and terminating procedures respectively.

Change

6.9 Description of subscriber data

6.9.1 Application Server subscription information

The Application Server Subscription Information is the set of all Filter Criteria that are stored within the HSS for service profile for a specific user. This information shall be sent by the HSS to the S-CSCF via the Cx Interface during registration.

6.9.2 Filter Criteria

This clause defines the contents of the Filter Criteria. This information is part of the Application Server Subscription Information. For further information about the XML modelling see 3GPP TS 29.228 [8].

Filtering is done for initial SIP request messages only.

The S-CSCF shall apply filter criteria to determine the need to forward SIP requests to Application Servers. These filter criteria will be downloaded from the HSS. ~~The HSS shall provide filter criteria in the prioritized list.~~

Initial Filter Criteria (iFC) are stored in the HSS as part of the user profile and are downloaded to the S-CSCF upon user registration, or upon a terminating initial request for an unregistered user if unavailable. They represent a provisioned subscription of a user to an application. After downloading the User Profile from the HSS, the S-CSCF assesses the filter criteria ~~activates for the indicated Application Server the Service Points of Interest that are correlated to the iFC in the User Profile~~. Initial Filter Criteria are valid throughout the registration lifetime of a user or until the User Profile is changed.

Subsequent Filter Criteria (sFC) are not used in this version of this specification.

6.9.2.1 Application Server address

Address to be used to access the Application Server for a particular subscriber.

6.9.2.2 Default ~~IP multimedia~~ handling ~~procedure~~

The Default ~~IP Multimedia H~~handling procedure indicates whether to abandon matching of lower priority triggers and to release the dialogue ~~IP Multimedia session shall be released~~; or to continue~~d~~ the dialogue and trigger matching. ~~as requested in case that AS requests to perform the default handling procedure during the dialogue between AS and S-CSCF or of loss of communications between the S-CSCF and Application Server is failed~~.

Use of the default handling procedure by the AS is not supported in this version of this specification.

6.9.2.3 Trigger point

Trigger Points are the information the S-CSCF receives from the HSS that defines the relevant SPIs for a particular application. They define the subset of initial SIP requests received by the S-CSCF that should be sent or proxied to a particular application. When the S-CSCF receives an initial SIP request, it evaluates the filter criteria one by one. If the initial SIP request matches the filter criteria, the S-CSCF proxies the SIP request to the corresponding SIP AS/IM-SSF/OSA SCS.

6.9.2.4 ~~Application Server priority list~~iFC Priority

If there are multiple ~~application servers~~initial Filter Criteria ~~are~~ assigned for one subscriber, ~~a~~ the priority shall ~~be assigned to application servers which~~ describes the order in which the S-CSCF shall assess them, and then contact the Application Servers ~~in case a~~when the SIP request matches the initial filter criteria ~~of more than one application server~~.

In this case, the S-CSCF shall interact with the application server~~s~~ associated with the initial matching filter criteria, starting from the ~~application server,~~filter criteria which has the highest priority.

6.9.2.5 Service Information

~~Service Information is an optional part of a Filter Criteria, which is a string of information.~~ Service Information is transparent information, and is not processed by the HSS or the S-CSCF. Service Information is optionally part of an initial Filter Criteria. If it is available from the initial Filter Criteria the S-CSCF shall include it into the body of the SIP request which is sent from the S-CSCF to the AS to which the initial Filter Criteria is pointing to. ~~Service Information is not processed, analysed or evaluated by the S-CSCF.~~

6.9.3 Authentication data

This clause defines the Authentication Data. This data shall be sent by the HSS to the S-CSCF via the Cx Interface during registration.

For definition of authentication data see specification 3GPP TS 23.008 [10]. For the handling of authentication data, see 3GPP TS 33.203 [11].

Change

7.2 Interfaces defined for HSS

7.2.1 HSS – CSCF (Cx) interface

This interface is used to send subscriber data to the S-CSCF, including Filter Criteria (and their priority); ~~to the S-CSCF; including Filter criteria,~~ which indicates which SIP requests should be proxied to which Application Servers.

The protocol used between the HSS and CSCF (Cx Interface) is specified in 3GPP TS 29.228 [8].

Change

B.3 Example information flows for a voicemail service

B.3.1 User out of coverage message recording

Figure B.3.1.1 shows a possible scenario of an Application Server, which acting as a terminating UA performs the function of a Voicemail Server in order to terminate a call and record a message on behalf of a UE that is out of coverage or powered off.

A S-CSCF is forwarded the initial INVITE destined for a UE that is not currently IMS registered. The Default Filter Criteria in the S-CSCF indicates that for the case of an unregistered user the INVITE should be forwarded to the Voicemail and Announcement Server.

Upon receiving the INVITE request the Voicemail and Announcement Server determines that the destination UE has subscribed to the Voicemail Service (possibly by downloading some subscriber profile information via the Sh interface). The Voicemail and Announcement Server therefore in addition to playing an announcement to inform the caller that the called party is either powered off or out of coverage also informs the caller that he may leave a message for the called party.

The calling party leaves a message for the called party and then hangs up the call by sending a BYE.

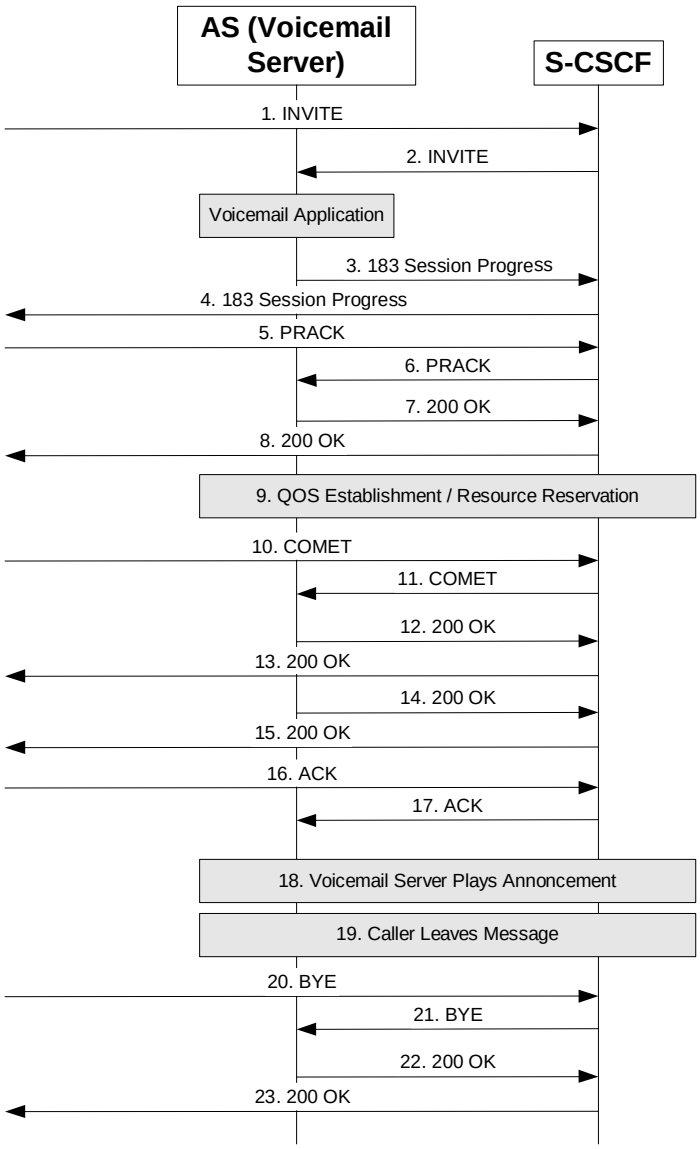


Figure B.3.1.1: Voicemail server records messages

Notes for figure B.3.1.1:

NOTE: For simplicity the 100 Trying response returned or received by the S-CSCF in reponse to requests is omitted from figure B.3.1.1.

1) INVITE request destined for an unregistered user is received at the S-CSCF ~~from caller~~.

2) Based on ~~Default~~ trigger point of the initial Filter Criteria S-CSCF proxies the INVITE request to the AS (Voicemail ~~and Announcement~~ Server) ~~(AS).~~

3-4) The AS starts the voicemail application and responds with a 183 Session Progress containing SDP which is proxied back to the caller by the S-CSCF.

5-8) The caller responds with a PRACK containing SDP, which the S-CSCF proxies to the AS and the AS responds with a 200 OK containing SDP which the S-CSCF proxies back to the caller.

QOS establishment and resource reservation takes place.

10-13) After completing resource reservation the caller sends a COMET containing SDP which is proxied by the S-CSCF to the AS which responds with a 200 OK containing SDP which is proxied back to the caller by the S-CSCF.

14-15) The AS then sends a 200 OK to the initial INVITE which the S-CSCF proxies to the caller.

16-17) The caller returns an ACK to the 200 OK.

18) The AS plays an announcement using the session established indicating that the caller is powered off but that the caller may leave a message.

19) The caller leaves a message using the session established.

20-21) The caller hangs up by sending a BYE which the S-CSCF proxies to the AS.

22-23) The AS responds with a 200 OK, which the S-CSCF proxies back to the caller.

3GPP TSG-CN1 Meeting #24
Budapest, Hungary, 13th – 17th May 2002

Tdoc N1-021424

CR-Form-v5

CHANGE REQUEST

⌘ **23.218** **CR** **017** ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification to Handling of IP multimedia registration for barred public user identities
Source:	⌘	dynamicsoft
Work item code:	⌘	IMS-CCR
Date:	⌘	04.05.2002
Category:	⌘	**F**
Release:	⌘	REL-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	SA2 agreed that public user identities may be barred including temporary public user identities derived from a USIM.
Summary of change:	⌘	Clarification that the contents of the To header in the third party register request sent to an AS should be based on the public user identity in the filter criteria trigger.
Consequences if not approved:	⌘	Ambiguity in the specification regarding S-CSCF behaviour at registration regarding handling of Filter Criteria and barred public user identities.

Clauses affected:	⌘	6.3		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	24.229, 23.218 (CR XX), 23.228 (CR XX)
Other comments:	⌘			

6.3 Handling of IP multimedia registration

Upon receiving the initial registration request from the user, the S-CSCF shall authenticate the user and upon receiving a subsequent registration request containing valid authentication credentials, download the user profile from the HSS. For further detailed information on registration and authentication procedures see 3GPP TS 24.229 [5] and 3GPP TS 33.203 [11].

After a successfully authenticated registration, the S-CSCF shall download from the HSS all the implicitly registered public user identities associated with the registered public user identity and the S-CSCF shall then determine based on the filter criteria information downloaded from HSS which application servers to inform about the registration event of the public user identity(s). If the registration request matches the filter criteria of some application servers, the S-CSCF needs to inform the application servers by performing a third party registration to the those application servers which are interested to be informed about the user registration event of these public user identities.

The important information carried in the third party REGISTER request is the public user identity, the S-CSCF address and the expiration time. It shall be possible based on operator configuration to use one of the implicitly registered public user identities as the public user identity in the To: header of the third party REGISTER request sent to the Application Server. Additional application server specific data, which is associated with the Filter Criteria and obtained from the HSS, is added to the REGISTER request body. This data should include the IMSI for an Application Server that supports CAMEL services or the private user identity for other Application Servers as received from the HSS.

This third party registration will include an expiration time that is equal to the expiration time sent to the UE by the S-CSCF in the 200 OK response to the incoming REGISTER request

On receiving a failure response to one of the REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the initial Filter Criteria. If the filter criteria does not contain an instruction to the S-CSCF regarding the failure to contact the Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

See figure 6.3.1:

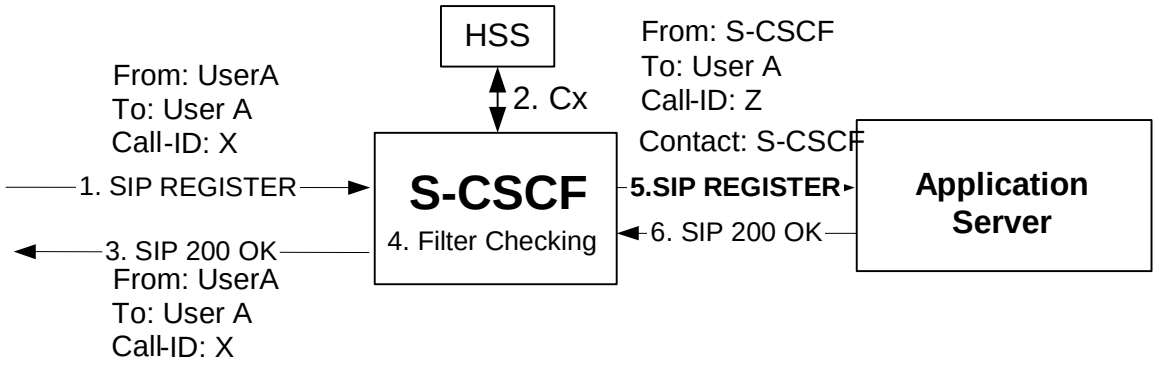


Figure 6.3.1: S-CSCF handling registration

Application Servers can in addition subscribe to the S-CSCF Registration Event Package. This provides a mechanism for the Application Server to discover all the implicitly registered public user identities without requiring multiple Register requests to be sent to the Application Server. The S-CSCF will send NOTIFY requests to the Application Server that has subscribed to the registration event package for the registered public user identity.

More information on these procedures is contained in 3GPP TS 24.229 [5].

3GPP TSG-CN1 Meeting #24
Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021441

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **115** ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Support for ISIM-less UICC
Source:	⌘	Ericsson, Vodafone
Work item code:	⌘	IMS-CCR
Date:	⌘	15-May-02
Category:	⌘	**B**
Release:	⌘	REL-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	There is not support for UICCs that do not contain the ISIM application
Summary of change:	⌘	Addition of a pointer to 23.003 in the case the UICC does not contain the ISIM application. Clarification that the S-CSCF gets barred and non-barred implicitely public user identities from the HSS. Only the non-barred IDs are bound to the Contact. Clarification that the S-CSCF does not send the barred public user IDs in the NOTIFY. Addition of the S-CSCF barring an attempt to initiate or terminate a session with a barred public ID.
Consequences if not approved:	⌘	Only UICCs that contain the ISIM applicationwill work with IMS

Clauses affected:	⌘	3.2, 4.2, 5.1.1.,5.2.2, 5.4.2.1.2, 5.4.3.1, 5.4.3.2		
Other specs affected:	⌘	**X** Other core specifications	⌘	23.003, 24.228
		☐ Test specifications		
		☐ O&M Specifications		
Other comments:	⌘	Part of the functionality introduced by this CR is implemented in CR 060		

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

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

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

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

FIRST PROPOSED CHANGE

3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AS	Application Server
AUTN	Authentication TokeN
BGCF	Breakout Gateway Control Function
c	conditional
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
i	irrelevant
I-CSCF	Interrogating CSCF
IMSI	International Mobile Subscriber Identity
IK	Integrity Key
IM	IP Multimedia
IP	Internet Protocol
ISC	IP multimedia Subsystem Service Control
ISIM	IMS Suscriber Identity Module
m	mandatory
MAC	Message Authentication Code
MGCF	Media Gateway Control Function
MRFC	Media Resource Function Controller
n/a	not applicable
o	optional
P-CSCF	Proxy CSCF
PDU	Protocol Data Unit
RAND	RANDom challenge
RES	RESponse
RTP	Real-time Transport Protocol‘
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SQN	SeQuence Number
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Universal Resource Identifier
USIM	UMTS Subscriber Identity Module
URL	Universal Resource Locator
x	prohibited

NEXT PROPOSED CHANGE

4.2 URL and address assignments

In order for SIP and SDP to operate, the following preconditions apply:

1) I-CSCFs used in registration are allocated FQDNs. Other IM CN subsystem entities may be allocated FQDNs. How these addresses are assigned to the logical entities is up to the network operator. For example, a single FQDN may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or a separate FQDN may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

Editor's note: The requirements for DNS-SRV entries or alternatives require further discussion.

2) All IM CN subsystem entities are allocated IP addresses. Allocation of IPv6 and IPv4 addresses fulfils the requirements of of 3GPP TS 23.221 [6] subclause 5.1.

3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the ISIM application, if present, on the UICC. Where no ISIM application is present, the private user identity is derived from the IMSI, which is contained on the USIM (see 3GPP TS 23.003 [3]). This private user identity is available to the SIP application within the UE.

NOTE: The FQDNs may be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

4) The subscriber is allocated one or more public user identities by the home network operator. At least one of these is contained within the ~~USIM~~ISIM application, if present, on the UICC. Where no ISIM application is present, the UE shall derive a temporary public user identity from the IMSI contained on the USIM (see 3GPP TS 23.003 [3]). All registered public user identities are available to the SIP application within the UE, after registration.

5) The UE is dynamically assigned an IP version 6 address.

NEXT PROPOSED CHANGE

5 Application usage of SIP

5.1 Procedures at the UE

5.1.1 Registration and authentication

5.1.1.1 General

The UE shall register public user identities (see table A.3/1 and dependencies on that major capability).

In case a UE registers several public user identities at different points in time, the procedures to re-register, deregister and subscribe to the registration-state event package for these public user identities can remain uncoordinated in time.

5.1.1.1A Parameters contained in the UICC

In case the UE is loaded with a UICC that contains the ISIM application, it will be preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one ore more public user identities; and
- the home network domain name used to address the SIP REGISTER request

In case the UE is loaded with a UICC that does not contain the ISIM application, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003 [3].

The temporary public user identity is only used in REGISTER requests. After a successful registration, the UE will get the associated public user identities, and any of them shall be used in subsequent non-REGISTER messages.

As the temporary public user identity may be barred, the UE shall not ~~indicate~~reveal ~~to the user~~ the temporary public user identity to the user.

In the case the UE needs to derive the temporary public user identity, the procedure shall be executed every time the UICC is changed.

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists.

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [14], received in an earlier registration.

The public user identity to be registered can be extracted either from the ISIM application, if present, on the UICC~~SIM~~ or derived from the USIM, according to the procedures described in subclause 5.1.1.1A. ~~If no ISIM is present, the UE shall use the temporary public user identity derived the temporary public user identity from the IMSI contained on the~~

~~USIM.~~ ~~or~~ A public user identity may be input ~~from~~ by the end user. On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity~~. This shall be extracted from the ISIM application, if present, contained on the UICC. If no ISIM application is present, the private user identity id derived from shall be extracted from the IMSI contained on the USIM (see 3GPP TS 23.003[3])~~;

b) the From header shall contain ~~the temporary public user identity, derived from the IMSI contained on the USIM (see 3GPP TS 23.003 [3]) or shall contain~~ the public user identity to be registered;

c) the To header shall contain ~~the temporary public user identity, derived from the IMSI contained on the USIM (see 3GPP TS 23.003 [3]) or shall contain~~ the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, shall contain 600 000 seconds as the value desired for the duration of the registration;~~.~~

e) a Request-URI that contains the SIP URI of the domain name of the home network.

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

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

The use of the Path header shall not be supported by the UE.

On receiving the 200 OK response to the REGISTER request, the UE shall store the expiration time of the registration.

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

On receiving a 423 Registration too brief response to the REGISTER request, the UE shall:

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

5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the users registration-state event package for the public user identity registered as described in subclause 5.1.1.2 at the users registrar (S-CSCF). Therefore the UE shall generate a SUBSCRIBE request with the following elements:

- a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URL that contains ~~the~~ a public user identity ~~that was previously registered~~;
- a From header set to a SIP URL that contains ~~the~~ a public user identity ~~that was previously registered~~;
- a To header, set to a SIP URL that contains ~~the~~ a public user identity ~~that was previously registered~~;
- an Event header set to the "registration-state" event package;
- an Expires header set to a value higher than the Expires header of the before sent REGISTER request.

Afterwards it shall send out the so generated SUBSCRIBE request.

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

The UE shall automatically resubscribe to the registration-state event package for a previously registered public user identity if the expiration time, as indicated in the Expires header of the 2xx response to the SUBSCRIBE message, has run out and the public user identity is still registered.

NEXT PROPOSED CHANGE

5.2 Procedures at the P-CSCF

5.2.1 General

The P-CSCF shall support use of the Path header.

NOTE: The Path header is only applicable to the REGISTER request and its 200 OK response.

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE ~~that pertains to a given public user identity~~, the P-CSCF shall:

- insert a Path header in the request. The P-CSCF shall include in the Path header an entry containing the SIP URL identifying the P-CSCF;
- insert a Require header and a Proxy-Require header both containing the option tag "path";
- if the REGISTER request was received with a valid integrity check, add information to the REGISTER request to indicate that the REGISTER request was received with a valid integrity check; and

Editor's Note : The exact mechanism for this is FFS.

- 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) remove its SIP URL from the list of Path headers, reverses the order of the list and save the resulting list of Path headers. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routeing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing Path headers with the new list;
2) associate the Path header information with the registered public user identity;
3) remove the list of Path headers and "path" option-tags from the 200 OK response before forwarding the response to the UE.

When the P-CSCF receives a 401 Unauthorized response to a REGISTER request, the P-CSCF shall remove and store the CK and IK values contained in the 401 Unauthorized response. The 401 Unauthorized response shall be forwarded to the UE if and only if the CK and IK have been removed.

Editor's Note: The P-CSCF behaviour when 3xx or 4xx responses other than 401 Unauthorized are received is FFS.

Editor's Note: The text above assumes that public user identities are registered one by one. Public user identity might need to be changed to Service Profile in the case when public user identities can be implicitly registered.

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

When the P-CSCF receives a 420 Bad Extension response to the above REGISTER request, the P-CSCF shall check the value of the Unsupported header field. When the value of the Unsupported header field is path, the P-CSCF shall take OA&M actions to indicate an error, in addition to passing on the 420 response to the UE. In all other cases, the P-CSCF shall proxy the 420 Bad Extension response.

NEXT PROPOSED CHANGE

5.4.2.1.2 Notification about registration state

Notification of the registration state shall affects the non-barred public user identities. The barred public user identities ~~are~~shall never be sent in a NOTIFY message.

If the registration state of one or more non-barred public user identities changes, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the registration-state event package of that user. For each NOTIFY request, the S-CSCF shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value;
- indicate registration state "open" for all public user identities which are currently registered;
- indicate registration state "closed" for all public user identities which are currently deregistered; and
- indicate within the "<detail>" information of those public user identities which will be automatically reregistered the "automatically by" information, followed by the specific public user identity which will cover the reregistration.

EXAMPLE: If sip:user1_public1@home1.net is reregistered, the public user identity sip:user1_public2@home1.net was automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<tuple name="sip:user1_public1@home1.net">
  <status><value>open</value></status>
</tuple>

<tuple name="sip:user1_public2@home1.net">
  <status> <value>open</value> </status>
  <detail>automatically by sip:user1_public1@home1.net</detail>
</tuple>
```

Afterwards the S-CSCF shall send the generated NOTIFY request on the dialog and await a 2xx response.

NEXT PROPOSED CHANGE

5.4.3.1 Requests initiated by the served user

When the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

- determine whether the request contains a barred public user identity in the From or Remote-Party-ID header fields of the request or not. In case any of the said header fields contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps.

- remove its own SIP URL from the topmost Route header;

- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [16]) to a globally routable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [18]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or an appropriate SIP response shall be sent to the originator;

- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;

- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous check, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and

  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.

- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;

- determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI; and

- in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed.

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

- remove its own URL from the topmost Route header;

- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and

- route the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- route the request based on the topmost Route header.

NEXT PROPOSED CHANGE

5.4.3.2 Requests terminated at the served user

When the S-CSCF receives, destined for the served user, an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

- remove its own URL from the topmost Route header;
- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. In case of contacting one or more application server(s) the S-CSCF shall:
  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2.1;
- determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2.1;
- build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];
- insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed;
- replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- forward the request based on the topmost Route header.

When the S-CSCF receives a request destined for a barred public user identity, the S-CSCF shall return an appropriate unsuccessful SIP response. This response may be, e.g., a 404 (Not found) or 604 (Does not exist anywhere).

3GPP TSG-CN1 Meeting #24 ***Tdoc N1-021461***
Budapest, Hungary, 13. – 17. May 2002 **revision of N1-021445 (N1-021329)**

CR-Form-v5

CHANGE REQUEST

⌘ **23.003** **CR** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Use of a temporary public user identity
Source:	⌘	Vodafone, Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	1st May 2002
Category:	⌘	**F**
Release:	⌘	REL-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	SA2 have agreed the stage two for IMS access with a R99/Rel-4 USIM. In order to align with the stage two, it is now necessary to add the procedures to derive domain name, private user identity and public user identity from the IMSI.
Summary of change:	⌘	Addition of conversion procedures in a new section on IMS.
Consequences if not approved:	⌘	Pre-Release-5 USIMs not supported by IMS

Clauses affected:	⌘			
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ 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/3G_Specs/CRs.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.

1.1 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 TS 21.905: "3G Vocabulary".

[2] 3GPP TS 23.008: "Organization of subscriber data".

[3] Void.

[4] 3GPP TS 23.070: "Routeing of calls to/from Public Data Networks (PDN)".

[5] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[6] 3GPP TS 29.060: "GPRS Tunnelling protocol (GPT) across the Gn and Gp interface".

[7] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[8] GSM 09.03: "Digital cellular telecommunications system (Phase 2+); Signalling requirements on interworking between the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) and the Public Land Mobile Network (PLMN)".

[9] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

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

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

[12] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land Mobile Stations in public land mobile networks (PLMN)".

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

[14] RFC 791: "Internet Protocol".

[15] RFC 1883: "Internet Protocol, Version 6 (IPv6) Specification".

[16] 3GPP TS 25.401: "UTRAN Overall Description".

[17] 3GPP TS 25.413: "UTRAN Iu Interface RANAP Signalling".

[18] RFC 2181: “Clarifications to the DNS Specification”.

[19] RFC 1035: “Domain Names - Implementation and Specification”.

[20] RFC 1123: “Requirements for Internet Hosts -- Application and Support”.

[21] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes".

[22] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2"

[23] RFC 2486: "The Network Access Identifier"

[24] RFC 3261: "SIP: Session Initiation Protocol"

[25] 3GPP TS 31.102: "Characteristics of the USIM Application."

[26] RFC 1035: "Domain names – inplementation and specification"

*** Proposed New Section ***

13 Numbering, addressing and identification within the IP multimedia core network subsystem

13.1 Introduction

This clause describes the format of the parameters needed to access the IP mulimedia core network subsystem. For further information on the use of the parameters see 3GPP TS 23.228 [22].

13.2 Home network domain name

The home network domain name shall be in the form of an Internet domain name, e.g. operator.com, as specified in RFC 1035 [26].

If there is no ISIM application, the UE shall derive the home network domain name from the IMSI as described in the following steps:

1. remove any non-decimal digits from the IMSI, leaving a string of 15 or less digits;
2. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [25]) and separate them into MCC and MNC with "."; and
3. reverse the order of the MCC and MNC. Append to the result: ".IMSI.3gppnetwork.org"

An example of a home network domain name is:

EXAMPLE: IMSI in use: 234150999999999;

where;

MCC: 234;

MNC: 15;

MSIN: 0999999999; and

home domain name: 15.234.IMSI.3gppnetwork.org.

13.3 Private user identity

The private user identity shall take the form of an NAI, and shall have the form user@realm as specified in clause 3 of RFC2486 [23].

NOTE: It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

If there is no ISIM application, the private user identity is not known. In this case, the private user identity is derived from the IMSI.

The following steps show how to build the private user identity out of the IMSI:

1. remove any non-decimal digits from the IMSI, leaving a string of 15 or less digits;
2. use the result from step 1, i.e. the whole string of digits, as the user part of the private user identity; and
3. the first digits of the IMSI, i.e. MNC and MCC, will be converted into a domain name, as described in subclause 13.1.

The result will be a private user identity of the form imsi@mnc.mcc."IMSI.3gppnetwork.org". For example: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the private user identity then takes the form 234150999999999@15.234.IMSI.3gppnetwork.org

13.4 Public user identity

The public user identity shall take the form of either a SIP URI, see RFC3261[24] or an E.164 number. A SIP URI shall take the form "sip:user@domain".

In case there is no ISIM application to host the public user identity, a temporary public user identity shall be derived, based on the IMSI. The temporary public user identity shall be of the form "user@domain" and shall therefore be equal to the private user identity. The private user identity is derived as per subclause 13.2. That is, the private user identity will be appended to the string "sip:"

EXAMPLE: "sip:234150999999999@15.234.IMSI.3gppnetwork.org".

3GPP TSG-CN1 Meeting #24 **Tdoc N1-021208**
Budapest, Hungary, 13. – 17. May 2002

Source:	Nortel Networks
Title:	Restrict mobile use of the SGNSR bit for EDGE
Agenda item:	5
Document for:	DISCUSSION / APPROVAL

Discussion

In August 1999, CN1 sent a liaison to SMG2 requesting that SMG2 define a bit on the GSM BCCH who's primary purpose was to allow mobiles to know whether to use L3 MSC message numbering scheme, modulo 4, or L3 MSC message numbering scheme, modulo 2. Additionally, CN1 stated the possibility of using this bit to control the encoding used by the mobile even though this capability had not been required in previosus versions of DTAP signalling. Therefore, CN1 requested SMG2 define a bit on the BCCH, which would broadcast to the mobiles the revision of the core network. SMG2 defined two bits on the BCCH: MSCR (for Circuit-Switched Core Network) and SGSNR (for Packet-Switched Core Network).

At the CN1 #22 meeting, it was agreed that it is allowed for the MS to look at the CN revision and not initiate the secondary PDP context activation or PDP context modification procedures at all towards a pre-R99 CN.

However, for commercial reasons, operators and network manufacturers may want to introduce support of some R99 procedures before others on their pre-R99 networks. This provides the flexibility to allow rapid introduction of the features with the highest demand in the market place, and reduces the time to market for these commercially important features. The standards should be sufficiently flexible to meet this practical deployment requirement. Prior to release 99 the DTAP signalling met this requirement very well without the use of a network revision level indication.

The use of two bits to represent the MSC and the SGSN revision level by mobiles restricts the ability to make early introduction of R99 features. This is particularly true because the precise handling of the MSCR and SGSNR bit at the mobile is not defined and therefore actual mobile behaviour can only be determined by testing or bilateral discussion.

One particularly important R99 feature is the support of EDGE. The support of EDGE in a particular cell is indicated by very specific parameters in the GPRS Cell Options IE on the BCCH. In order to allow early introduction of EDGE it is proposed that mobiles should base their support for EDGE only on the indication provided in the specific EDGE BCCH bits and not on the SGSNR bit.

Proposal

Nortel requests CN1 agree:

- The MS shall NOT look at the SGSN revision bit to determine whether the SGSN supports EDGE. The MS shall only look at the GPRS Cell Options IE to determine whether EDGE is supported in the network or not.
- Send a Liaison to the relevant GERAN WG indicating the CN1 agreement.

In addition Nortel suggests CN1 discuss whether the use of two bits to indicate all aspects of the MSC and SGSN revision level is appropriate. More flexibility may be provided by using the approach of "attempt and detect failure", used in previous versions of DTAP, or possibly a separate version control for different packages, used in MAP.

3GPP TSG-CN1 SIP Rel-5 Ad Hoc Meeting ***Tdoc N1-020985***
Madrid, Spain 23. - 25. April 2002

Source: Lucent Technologies

Title: MRFC interface details

Agenda item: 7.10

Document for: DISCUSSION

Introduction

The details of the MRFC interface with the AS (via the S-CSCF) are currently described as FFS. If the details for the basic operations are not defined, then only proprietary solutions will be available in Rel-5. This paper outlines an approach to define this interface. Separate contributions will suggest the specific changes to 3GPP TS 24.229.

Discussion

The following issues need to be resolved for the AS interface to the MRFC (via the S-CSCF) to request services and to discover MRFC capabilities. There is an assumption to reuse as much standard SIP and SDP as possible.

1. Will the AS always direct requests to a specific MRFC or will the AS be allowed to specify a generic MRFC that must be resolved by the S-CSCF?
   The former will always be needed because of the subsequent requests and may also be the only initial method. The latter should be considered as an optional function of the S-CSCF, where the AS will either know it can try this ahead of time or learn about it through trial and error.
2. How will the AS/S-CSCF discover MRFC and its capabilities?
   There are several choices including configuration (static and HSS stored), IETF discovery protocols and the OPTIONS method within SIP. Only the OPTIONS method would be described within 24.229. The OPTIONS request may need to be sent to the MRFC from both the AS and S-CSCF. However, the S-CSCF would only need to do this if it supported the generic MRFC option. The other part of the discussion is whether an AS may need to send an OPTIONS request to an MGCF within a dialog to be able to attempt some optimization cases for conferencing or tones/announcements.
3. What mechanism will the AS use to specify requested services? (e.g. SIP URI parameters, SIP headers or XML message body)
   The choices of mechanisms have the following characteristics.
   - The SIP URI parameters (or standard SIP headers) would be the most efficient and perhaps could be the most common with generic solutions in the long term. However, it requires strict IETF standardization, which may not happen in time for Rel-5, and will leave no room for 3GPP specifics.
   - The P-header option would allow more flexibility in passing 3GPP specific data in a header, which is presumably more efficient than using a message body. Although the details would be included in an informational IETF document, it appears that the IETF SIP group would still exert some control over what could be defined and would need to approve any changes too (similar concerns on whether it can be accomplished in Rel-5 timeframe).
   - The XML message body is the most flexible option for 3GPP to have complete control over the content. But there is some concern over performance, size of message. Both this and the P-header option also may hinder future commonality with other solutions.

This paper covers four areas related to the MRFC interface with the AS (via the S-CSCF).

1. Basic call scenario support for tones, announcements, transcoding, and conference calls. This includes a description of how to pass instructions for the requested function using XML within the message body.
2. Using the OPTIONS request to return MRFC (and MGCF) capabilities to the AS. There is also a mention of the MRFC discovery options.
3. Optimising the signalling when tones/announcements are needed for existing session that it is using and MRFP (or MGW), assuming that the same MRFP (or MGW) gets used for playing the tone/announcement.
4. Option of having AS send request using a generic MRFC request URI.

The following diagram illustrates the signalling paths from the AS to the MRFC for call scenarios and for requesting MRFC capability information. For any given call scenario, one of the AS entities may be in communication with one of the S-CSCF entities to get to one of the MRFC entities. In many cases the AS is a SIP UA; it may also be a SIP proxy. The MRFC is a SIP UA. The S-CSCF is a SIP proxy and can be viewed as an outbound proxy for the AS.

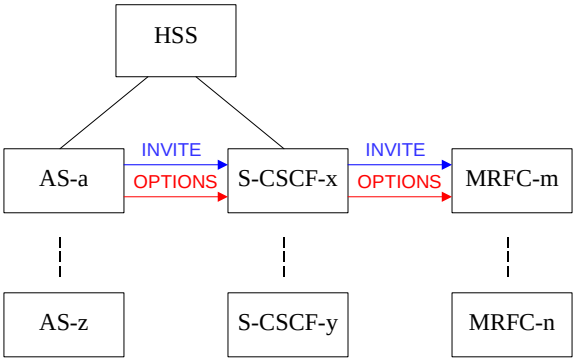


Figure 1: AS signalling paths to MRFC

The following sub-sections further describe each of the four areas to consider.

Call scenarios to request resources and invoke capabilities

Refer to 23.218 for possible call scenarios for tones/announcements, transcoding and ad hoc conferences where the AS is a B2BUA.

Tones

Tones are defined in Packages in H.248/MEGACO. H.248/MEGACO defines base packages that can be extended. Packages are identified with Package Name and Package ID, and they are registered with IANA. It is also possible to specify files to use from a server to play a tone.

For tone generation packages, tones are defined as individual signal. The general attributes for signals are: Signal Name, Signal ID (tone id), Type (Brief, TimeOut, OnOFF), and Duration (Provisioned, Not Audible, etc.). There are also optional Additional Parameters defined for signals, such as Tone Direction (which is defined by Parameter ID, Type (enum, ...), Values (external, internal, both), and Default).

For requesting to play a tone at MRFC/MRFP, it should be sufficient for the AS to indicate Package ID, Signal Name and/or Signal ID, and values for additional parameters when applicable. Alternatively, a file name may be specified.

Table 1. Summary of Tone Packages for H.248/MEGAGO

Origin	Package Name	Package ID	Descriptions	
H.248/MEGACO Base Packages	Tone Generator	tonegen (0x0003)	- defines signals to generate audio tones. - MGs are expected to be provisioned with the characteristics of appropriate tones for the country in which the MG is located.	
	Tone Detection	tonedet (0x0004)	- defines events for audio tone detection. - Tones are selected by name (tone id)	
	Basic DTMF Generator	dg (0x0005)	- defines the basic DTMF tones as signals - extends the allowed values of parameter tl of playtone in tonegen. No additional pameters.	
	DTMF detection	dd (0x0006)	- defines the basic DTMF tones detection. - extends the possible values of tone id in the "start tone detected" "end tone detected" and "long tone detected" events	

	Call Progress Tones Generator	cg (0x0007)	- defines the basic call progress tones as signals, e.g. dial tone, ringing tone, busy tone, congestion tone, payphone recognition tone, call waiting tone, caller waiting tone. No additional parameters. - extends the allowed values of the tl parameter of playtone in tonegen	
	Call Progress Tones Detection	cd (0x0008)	defines the basic call progress detection tones	
	Analog Line Supervision	al (0x0009)	defines events and signals for an analog line e.g. onhook, offhook, flashhook	
draft-boyle-megaco-tonepkgs-07 "Supplemental Tones Packages for Megaco/H.248"	Conferencing Tones Generation	conftn (0x0038)	defines conferencing signals, e.g. Conference Entrance Tone Conf. Exit Tone Conf. Lock Tone Conf. Unlock Tone Time Limit Warning Tone	
	Diagnostic Tones Generation	test (0x0039)	defines diagnostic signals for use by telephony providers, e.g. Low Tone, High Tone, Loud Tone, Faint Tone, Slow Interrupted Tone, Fast Interrupted Tone	
	Carrier Tones Generation	carr (0x003a)	defines signals for use by carrier services, e.g., Carrier Dial Tone, Carrier Answer Tone, Carrier Charging Tone, Long Distance Ind. Tone	
draft-bothwell-megaco-mftonepkgs-03 "MF Tone Generation and Detection Packages"	Multi-Frequency Tone Generation	mfg (0x003d)	- defines the basic MF tones as signals and - extends the allowed values of parameter t1 of playtone in tonegen. Signals defined: MF signal code 0, code 1, …	
	Multi-Frequency Tone Detection	mfd (0x003e)	defines the events required for basic MF tone detection	
ITU-T Q.1950 (for CBC)	Basic Call Progress Tones Generator with Directionality	Bcg 0x0023		
	Expanded Call Progress Tones Generator	Xcg 0x0024	defines additional call progress indications as signals and allows for specification of directionality, e.g. comfort tone, off-hook warning tone, neg ack tone, vacant number tone, special condition dial tone	
	Basic Services Tones Generation	Srvtn 0x0025	defines signals for use by telephony services and allows for specification of directionality. E.g. recall dial tone, confirmation tone, held tone, message waiting tone	
	Expanded Services Tones Generation	Xsrvtn 0x0026	e.g. call transfer dial tone, call forward tone, credit card service tone, special recall dial tone	

	Intrusion Tones Generation	Int 0x0027	e.g, intrusion pending tone, intrusion tone, intrusion reminder tone, toll break in tone, intrusion queue tone, busy verification tone	
	Business Tones Generation	Biztn 0x0028	e.g. off-hook queuing tone, expensive route warning tone, distinctive dial tone, internal dial tone	

Announcements

Announcements may be requested from H.248/MEGAGO packages at the MRFC/MRFP. Annex K of H.248 describes the support for fixed and variable announcements, but no specific announcements are defined.

It is also possible for the AS to identify files on a server for the MRFC/MRFP to play an announcement.

Transcoding

For transcoding it should be sufficient to identify the codecs using SDP.

Optionally, it may also be reasonable to treat transcoding as a two-party conference call. If this is done, then a transcoding session could be easily extended to a multiparty conference call if a resource identifier is assigned initially.

Conference Calls

Multiparty ad hoc conference calls require the assignment of a resource identifier for the conference facility so that parties may be added/subtracted from the conference. There also may be a need to communicate the maximum number of participants for the conference.

Other multiparty operations, such as splitting off two parties for a private conversation, need to have a mechanism to indicate such requests. The alternative is to have the AS manage these types of operations with simpler primitives to manipulate each leg of the conference call.

Examples for each mechanism

The following examples (using conferencing) illustrate that all mechanisms being considered are viable. For these examples it is assumed that the AS addresses its requests to a specific MRFC. The user part of the Request URI will indicate the requested service and the domain name is a specific MRFC target destination to provide the service. The AS will need to discover the MRFC via some mechanism (perhaps HSS) and will need to query it for capabilities (e.g. OPTIONS request) if not included as part of the discovery mechanism.

Example requests for services:

Example 1 uses request URI parameters.

```
INVITE sip:conference@mrfc12.provider.com;max-participants=6 SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: <sip:conference@mrfc12.provider.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

and here is the response to the INVITE from the MRFC that uses contact for conference id

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP mrfc12.provider.com;branch=z9hG4bKnashds8
 ;received=192.0.2.3
Via: SIP/2.0/UDP s-cscf.provider.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
```

```
 ;received=192.0.2.1
To: <sip:conference@mrfc12.provider.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:mrfc12-conf-id-123456abc@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131

(MRFC's SDP not shown)
```

and here is a subsequent INVITE to join the same conference

```
INVITE sip: mrfc12-conf-id-123456abc@192.0.2.4 SIP/2.0
Via: SIP/2.0/UDP pc22.chicago.com;branch=z989asc09g97789s
Max-Forwards: 70
To: <sip:conference@mrfc12.provider.com>
From: Bob <sip:bob@chicago.com>;tag=6483921774
Call-ID: b8f89676e66710@pc22.chicago.com
CSeq: 540957 INVITE
Contact: <sip:bob@pc22.chicago.com>
Content-Type: application/sdp
Content-Length: 156

(Bob's SDP not shown)
```

Example 2 uses P-headers for parameters. The assumption here is that there is a generic P-header created for the MRFC, with indicator of type of service and various parameters.

```
INVITE sip:conference@mrfc12.provider.com SIP/2.0
P-3GPP-MRFC:service=conference;max-participants=6
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: <sip:conference@mrfc12.provider.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

and here is the response to the INVITE from the MRFC that uses P-header for conference id

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP mrfc12.provider.com;branch=z9hG4bKnashds8
 ;received=192.0.2.3
Via: SIP/2.0/UDP s-cscf.provider.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
 ;received=192.0.2.1
To: <sip:conference@mrfc12.provider.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
P-3GPP-MRFC:service=conference;conf-id=mrfc12-conf-id-123456abc
Contact: <sip:conference@192.0.2.4>
Content-Type: application/sdp
Content-Length: 131

(MRFC's SDP not shown)
```

and here is a subsequent INVITE to join the same conference

```
INVITE sip:conference@mrfc12.provider.com SIP/2.0
P-3GPP-MRFC:service=conference;conf-id=mrfc12-conf-id-123456abc
Via: SIP/2.0/UDP pc22.chicago.com;branch=z989asc09g97789s
Max-Forwards: 70
To: <sip:conference@mrfc12.provider.com>
From: Bob <sip:bob@chicago.com>;tag=6483921774
Call-ID: b8f89676e66710@pc22.chicago.com
CSeq: 540957 INVITE
Contact: <sip:bob@pc22.chicago.com>
Content-Type: application/sdp
Content-Length: 156

(Bob’s SDP not shown)
```

Example 3 uses XML message body for parameters.

```
INVITE sip:conference@mrfc12.provider.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: <sip:conference@mrfc12.provider.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: multipart/mixed; boundary=unique-boundary-1
Content-Length: 142

Unique-boundary-1

Content-Type: application/sdp

(Alice’s SDP not shown)

Unique-boundary-1

Content-Type: application/3gpp-ims-mrfc+xml

<ims-3gpp-mrfc version=”1.0”>
      <operation-request>
       <multiparty>
          <max-participants>6</max-participants>
       </multiparty>
     </operation-request>
</ims-3gpp-mrfc>
```

and here is the response to the INVITE from the MRFC that uses XML body for conference id

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP mrfc12.provider.com;branch=z9hG4bKnashds8
 ;received=192.0.2.3
Via: SIP/2.0/UDP s-cscf.provider.com;branch=z9hG4bK77ef4c2312983.1
 ;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
 ;received=192.0.2.1
To: <sip:conference@mrfc12.provider.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:conference@192.0.2.4>
Content-Type: multipart/mixed; boundary=unique-boundary-1
Content-Length: 131

Unique-boundary-1

Content-Type: application/sdp
```

```
(MRFC’s SDP not shown)

Unique-boundary-1

Content-Type: application/3gpp-ims-mrfc+xml

<ims-3gpp-mrfc version=”1.0”>
     <operation-response>
       <operation>multiparty</operation>
       <result>success</result>
       <resource-id>mrfc12-conf-id-123456abc</resource-id>
     </operation-response>
</ims-3gpp-mrfc>
```

and here is a subsequent INVITE to join the same conference

```
INVITE sip:conference@mrfc12.provider.com SIP/2.0
Via: SIP/2.0/UDP pc22.chicago.com;branch=z989asc09g97789s
Max-Forwards: 70
To: <sip:conference@mrfc12.provider.com>
From: Bob <sip:bob@chicago.com>;tag=6483921774
Call-ID: b8f89676e66710@pc22.chicago.com
CSeq: 540957 INVITE
Contact: <sip:bob@pc22.chicago.com>
Content-Type: multipart/mixed; boundary=unique-boundary-1
Content-Length: 156

Unique-boundary-1

Content-Type: application/sdp

(Bob's SDP not shown)

Unique-boundary-1

Content-Type: application/3gpp-ims-mrfc+xml

<ims-3gpp-mrfc version=”1.0”>
     <operation-request>
       <multiparty>
          <resource-id>mrfc12-conf-id-123456abc</resource-id>
       </multiparty>
     </operation-request>
</ims-3gpp-mrfc>
```

XML definition

Because XML alternative is under control of 3GPP, the following XML definition is suggested for communication with the MRFC. It will be identified with a new MIME type in the SIP Content-Type header. The associated MIME type with the 3GPP IMS XML body could be called "application/3gpp-ims-mrfc+xml".

The XML definition may look like the following.

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP IMS XML body used with the request to the MRFC. -->

<!DOCTYPE ims-3gpp-mrfc [
    <!-- ims-3gpp-mrfc element: root element -->

    <!ELEMENT ims-3gpp-mrfc (operation-request*, operation-response*, charging-id?)>
    <!ATTLIST ims-3gpp-mrfc version CDATA #REQUIRED>

    <!-- operation-request element: The MRFC operation requested -->
    <!ELEMENT operation-request     (tone | announcement | transcode | multiparty | dtmf | #PCDATA)>

    <!-- tone element: Tone operation -->
    <!ELEMENT tone                  (megaco-pkg-id?, private-pkg-id?, tone-id?, file?, duration?,
repeat?, delay?, direction?)>
```

```
    <!-- megaco-pkg-id element: optional MEGAGO/H.248 package identifier -->
    <!ELEMENT megaco-pkg-id         (#PCDATA)>

    <!-- private-pkg-id element: optional private package identifier -->
    <!ELEMENT private-pkg-id        (#PCDATA)>

    <!-- tone-id element: optional Tone Identifier -->
    <!ELEMENT tone-id               (#PCDATA)>

    <!-- file element: optional File identifier -->
    <!ELEMENT file                  (#PCDATA)>

    <!-- duration element: optional play duration time -->
    <!ELEMENT duration              (#PCDATA)>

    <!-- repeat element: optional value to repeat playing tone/announcement -->
    <!ELEMENT repeat>
    <!ATTLIST repeat
        value       (continuous | #PCDATA)>

    <!-- delay element: optional delay time before starting tone/announcement -->
    <!ELEMENT delay                 (#PCDATA)>

    <!-- direction element: optional tone/announcement direction identifier -->
    <!ELEMENT direction>
    <!ATTLIST direction
        value       (to_ue | to_far_end | both | #PCDATA)>

    <!-- announcement element: Announcement operations -->
    <!ELEMENT announcement          (megago-pkg-id?, private-pkg-id?, announcement-id?, file?, text?,
language?, duration?, repeat?, delay?, direction?, annc-params?)>

    <!-- announcement-id element: optional announcement identifier -->
    <!ELEMENT announcement-id       (#PCDATA)>

    <!-- text element: optional announcement text -->
    <!ELEMENT text                  (#PCDATA)>

    <!-- language element: optional announcement language identifier -->
    <!ELEMENT language              (#PCDATA)>

    <!-- annc-params element: optional announcement parameters -->
    <!ELEMENT annc-params           (#CDATA)>

    <!-- transcode element: Transcoding requests -->
    <!ELEMENT transcode             (resource-id?)>

    <!-- resource-id element: Identifier for MRFC transcoding or conference resource -->
    <!ELEMENT resource-id           (#PCDATA)>

    <!-- multiparty element: Multiparty (ad hoc conference) requests -->
    <!ELEMENT multiparty            (resource-id, max-participants?)>

    <!-- max-participants element: optional maximum participants for start of conference -->
    <!ELEMENT max-participants      (#PCDATA)>

    <!-- dtmf element: DTMF requests -->
    <!ELEMENT dtmf                  (send-or-collect, target, digits*)>

    <!-- send-or-collect element: indicate if sending or collecting DTMF digits  -->
    <!ELEMENT send-or-collect       (#PCDATA)>

    <!-- target element: send digits to this target (UE or far end), or collect digits from this
target (UE or far end)  -->
    <!ELEMENT target                (#PCDATA)>

    <!-- digits element: optional digits to send or that were received -->
    <!ELEMENT digits                (#PCDATA)>

    <!-- operation-response element: The response to the MRFC operation -->
    <!ELEMENT operation-response    (operation, result, resource-id?)>

    <!-- operation element: Identifier of operation -->
    <!ELEMENT operation>
    <!ATTLIST operation
        value       (tone | announcement | transcode | multiparty | dtmf | #PCDATA)>

    <!-- result element: MRFC result of operation -->
    <!ELEMENT result>
    <!ATTLIST result
        value       (success | failure | #PCDATA)>

    <!-- charging-id element: charging identifier -->
```

```
    <!ELEMENT charging-id          (#PCDATA)>
]>
```

MRFC discovery and returning capability information

When the AS is directing requests to a specific MRFC, it is preferable for the AS to have knowledge of MRFC/MRFP capabilities a priori. This may be used for either the initial request or for subsequent requests if additional functions are needed. As mentioned earlier, there are several possibilities for MRFC discovery and learning capabilities.

The OPTIONS method is a possible choice to use within SIP. The response to the OPTIONS request will contain an XML body that indicates the capabilities supported by the MRFC/MRFP. The OPTIONS request may include an XML body for the AS to ask about specific capabilities. The absence of this information means that the AS wants to retrieve information on all the capabilities of the MRFC/MRFP. See figure 2 for how this exchange would operate with the AS using the S-CSCF as an outbound proxy.

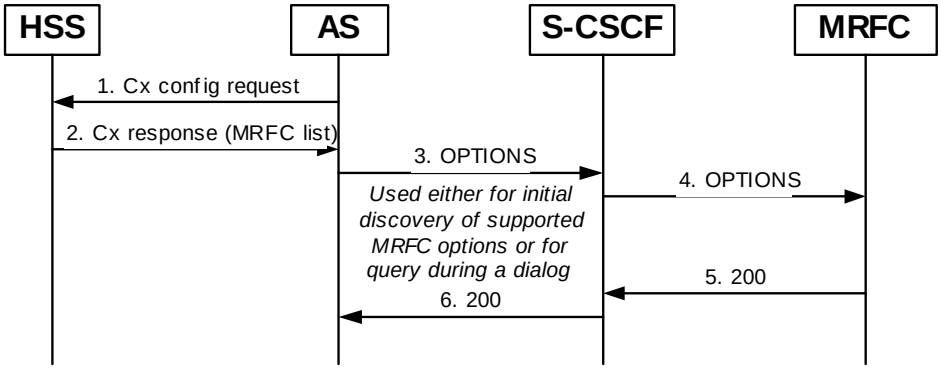


Figure 2: OPTIONS for MRFC

Figure 3 shows a related operation for the case of the AS querying for MGCF capabilities. This would be a prerequisite for the optimising function described later. For example, the AS wants to insert a tone or announcement for call between a UE and the PSTN.

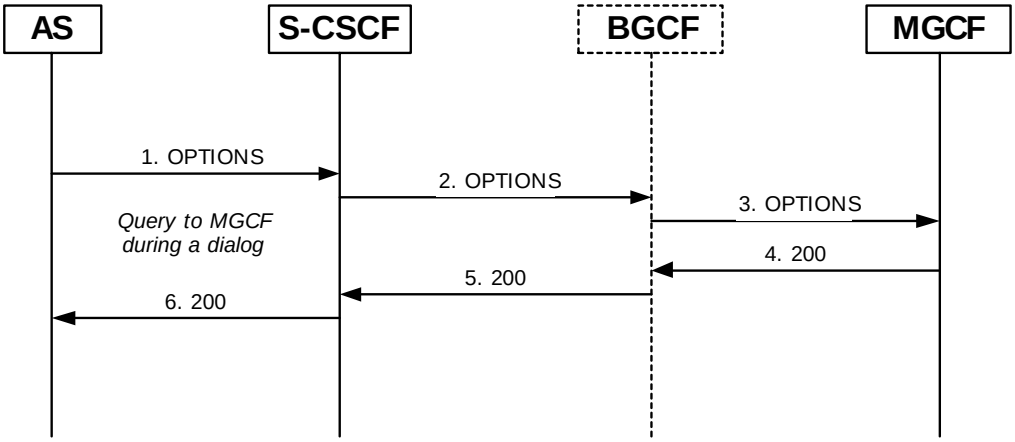


Figure 3: OPTIONS for MGCF

XML definition

This XML definition will be used when the AS needs to retrieve MRFC/MRFP capabilities to assist in choosing an appropriate MRFC to provide needed capabilities in a call scenario. The S-CSCF will need to use this if it makes the MRFC selection based on a generic request URI from the AS.

XML data, identified with a new MIME type in the SIP Content-Type header, is proposed as the mechanism for retrieving capabilities of the MRFC. The associated MIME type with the 3GPP IMS XML body is "application/3gpp-ims-

capabilities+xml". The XML definition may be shared for requesting MGCF/MGW capabilities, with a subset of the information applicable to the MGCF/MGW.

The XML definition may look like the following.

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP IMS XML body used with the OPTIONS request and response. -->

<!DOCTYPE ims-3gpp-capabilities [
    <!-- ims-3gpp-capabilities element: root element -->

    <!ELEMENT ims-3gpp-capabilities (network-entity, major-capabilities*, optional-packages*)>
    <!ATTLIST ims-3gpp-capabilities version CDATA #REQUIRED>

    <!-- network-entity element: The network entity of interest -->
    <!ELEMENT network-entity>
    <!ATTLIST network-entity
        value   (mrfc | mgcf | #PCDATA)>

    <!-- major-capabilities element: The major capabilities supported -->
    <!ELEMENT major-capabilities>
    <!ATTLIST major-capabilities
        value   (tone | announcement | transcoding | multiparty-call | dtmf | #PCDATA)>

    <!-- optional-packages element: The optional packages supported -->
    <!ELEMENT optional-packages (megaco-pkg-list | private-pkg-list | announcement-pkg-list |
multiparty-pkg-list | dtmf-list)>

    <!-- megaco-pkg-list element: list of MEGACO/H.248 defined packages -->
    <!ELEMENT megaco-pkg-list       (megaco-package-id*)>

    <!-- megaco-package-id element: megaco package identifier -->
    <!ELEMENT megaco-package-id     (#PCDATA)>

    <!-- private-pkg-list element: list of privately defined packages -->
    <!ELEMENT private-pkg-list      (private-pkg-id*)>

    <!-- private-pkg-id element: private package identifiers -->
    <!ELEMENT private-pkg-id        (#PCDATA)>

    <!-- announcement-pkg-list element: list of announcement optional packages -->
    <!ELEMENT announcement-pkg-list (language*, annc-bundle*)>

    <!-- language element: optional language identifier -->
    <!ELEMENT language              (#PCDATA)>

    <!-- annc-bundle element: optional announcement bundle identifier -->
    <!ELEMENT annc-bundle           (file-reference | #PCDATA)>

    <!-- file-reference: capability to retrieve announcement files from a server -->
    <!ELEMENT file-reference        (file-type+)>

    <!-- file-type: type of file understood -->
    <!ELEMENT file-type>
    <!ATTLIST file-type
        value   (wav | text | #PCDATA)>

    <!-- multiparty-pkg-list element: Multiparty calls (ad hoc conference) optional packages -->
    <!ELEMENT multiparty-pkg-list   (multiparty-bundle*)>

    <!-- multiparty-bundle element: Multiparty calls (ad hoc conference) bundle identifier -->
    <!ELEMENT multiparty-bundle (supported-operation | max-participants | #PCDATA)>

    <!-- supported-operation element: operations for managing conference -->
    <!ELEMENT supported-operation>
    <!ATTLIST supported-operation
        value   (member-primitives | mpty-functions | #PCDATA)>

    <!-- max-participants element: maximum number of participants supported per conference -->
    <!ELEMENT max-participants      (#PCDATA)>

    <!-- dtmf-list element: DTMF operations -->
    <!ELEMENT dtmf-list             (dtmf-function*)>

    <!-- dtmf-function element: DTMF functions -->
    <!ELEMENT dtmf-function
        value   (rtp-generate | rtp-collect)>

    ]>
```

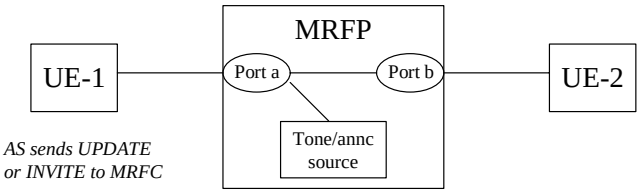
Optimising the signalling interface to MRFC when multiple capabilities requested

When an MRFC/MRFP is already involved for a dialog/session, it is desirable to use the same MRFC/MRFP when applying a tone/announcement to that dialog/session (assuming the MRFC/MRFP has that capability too). It is also preferable to do this with as few signalling messages as possible, which may be different than using the INVITE method.

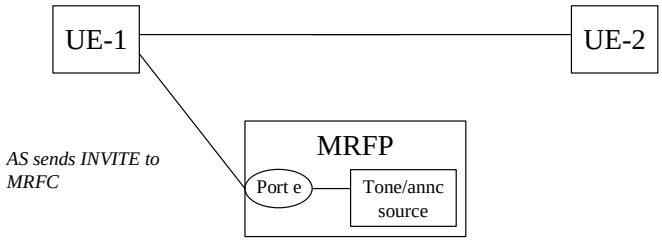
The diagrams below illustrate the possibilities of bearer paths when adding a tone/announcement to an existing point-to-point call or for a conference call. For cases 1a, 1b, 3 and 5 the bearer path is optimised and there is an opportunity to also optimise the signalling. The trade off to consider is some extra logic at the AS and MRFC to recognize the condition for optimising to get the benefit of fewer messages versus relying on the MRFC to recognize the opportunity to optimise the bearer path and using the benefit of one signalling sequence for requests.

For either UPDATE or INVITE, the same definitions for SDP and XML message bodies may be used.

Bearer path options for inserting tone/announcement into one side of point to point call.



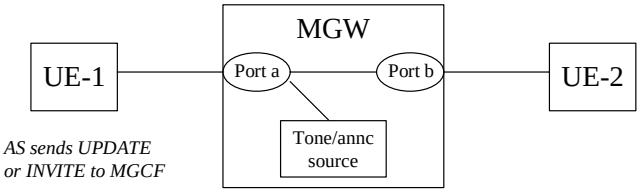
Case 1a: Always include MRFP with call setup to be prepared for changes to the session.



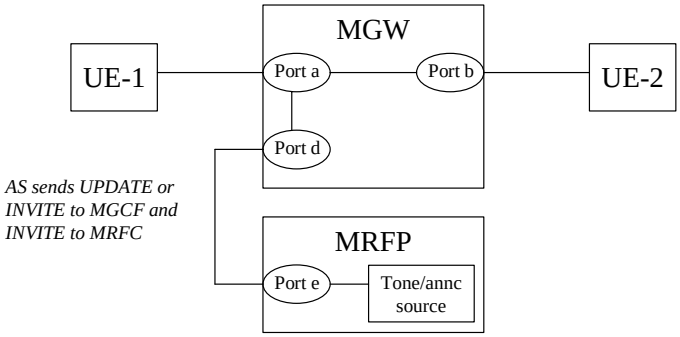
Case 2a: Include MRFP when necessary and try to minimize resource use. Same scenario could apply if MGW in path between between UE-1 and UE-2.

Figure 4: Bearer Path Options

Bearer path options for inserting tone/announcement into one side of point to point call.



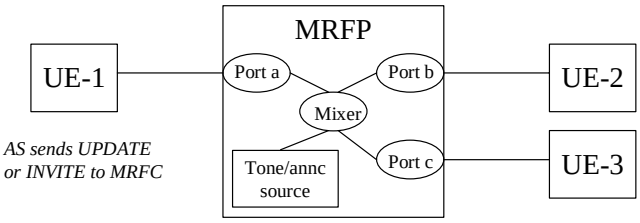
Case 1b: UE-2 is in circuit system and MGW has tone/announcement facilities.



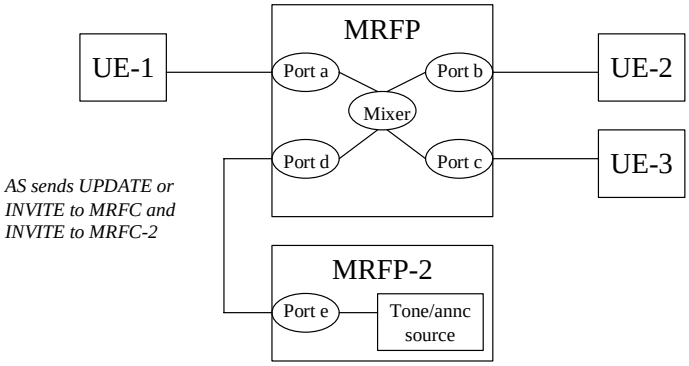
Case 2b: UE-2 is in circuit system and MGW does not have tone/announcement facilities.

Figure 5: Bearer Path Options (cont)

Bearer path options for inserting tone/announcement into multiparty call.



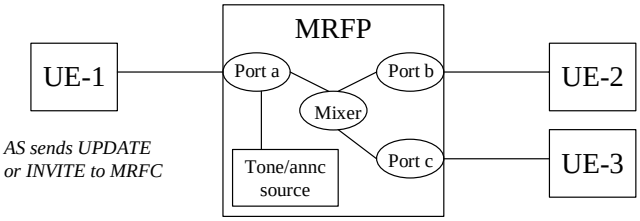
Case 3: All parties hear tone/announcement from one MRFP.



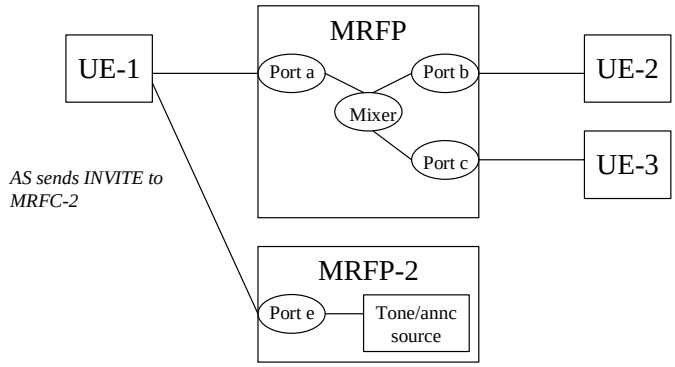
Case 4: All parties hear tone/announcement from second MRFP.

Figure 6: Bearer Path Options (cont)

Bearer path options for inserting tone/announcement into multiparty call.



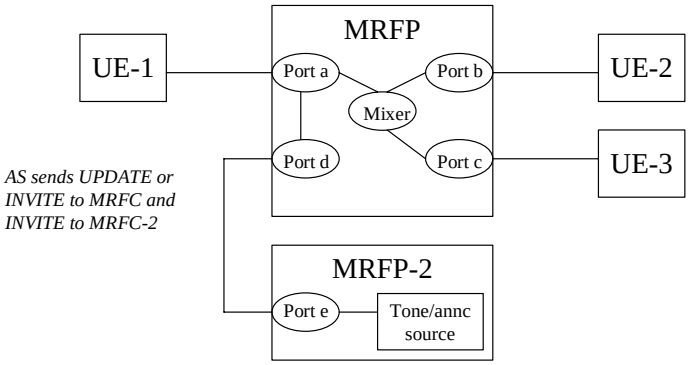
Case 5: One party hears tone/announcement from one MRFP.



Case 6: One party hears tone/announcement from second MRFP.

Figure 7: Bearer Path Options (cont)

Bearer path options for inserting tone/announcement into multiparty call.



Case 7: One party hears tone/announcement from second MRFP.

Figure 8: Bearer Path Options (cont)

Supporting call scenarios with generic MRFC request URI.

A useful function would be to have the AS make requests for services independent of what MRFC might be assigned to provide the service. (i.e. decouple the service request from the MRFC address) To accomplish this, there needs to be a configurable request URI to indicate the generic MRFC address to the AS and S-CSCF.

To provide this level of hiding from the AS, the S-CSCF will need to be able to assign an MRFC based on service request information in an INVITE and knowledge of MRFC capabilities. The OPTIONS method is the suggested way for the S-

CSCF to discover MRFC capabilities. The INVITE must use the same types of information as returned in the OPTIONS response to provide a matching mechanism for the S-CSCF. The HSS (AAA) will provide the list of possible MRFC entities for the S-CSCF to query capabilities. The AS may also use the HSS (AAA) interface to get this list. It may also be possible for the S-CSCF to provide the load balancing function when more than MRFC is available to provide a particular capability.

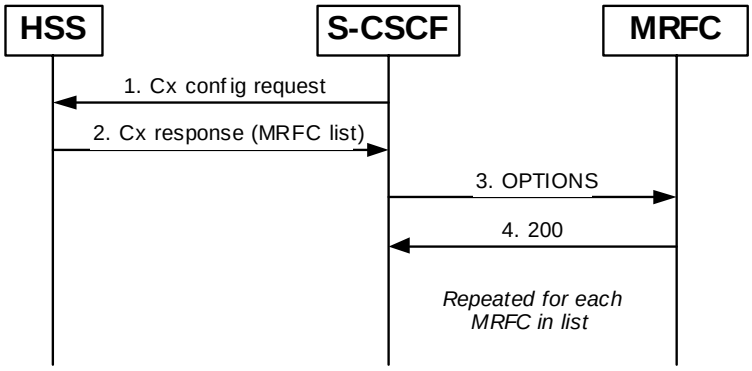


Figure 9: OPTIONS for MRFC from S-CSCF

The user part of the Request URI will indicate a generic MRFC address and either Request URI parameters, P-headers or XML message body may be used to indicate the requested service and further data for the request. IETF standardized Request URI parameters are preferred, but may not be available in Rel-5 timeframe. Under this scheme, the S-CSCF will be responsible for assigning an MRFC that can fulfil the request (and the S-CSCF may perform a load balancing function). The S-CSCF will either directly substitute the Request URI with the specific MRFC address or it will need to send a redirect back to the originator with the assigned MRFC. The S-CSCF will need to discover the MRFC via some mechanism (perhaps HSS) and will need to query it for capabilities (e.g. OPTIONS request) if not included as part of the discovery mechanism.

Example request for services using P-header:

```
INVITE sip:mrfc@provider.com SIP/2.0
P-3GPP-MRFC:service=conference;max-participants=6
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:mrfc@provider.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

Redirect (3xx) may be sent back with new Contact list pointing to specific MRFC to be used. Upon receiving the redirect, the AS would start a new INVITE with the same options as described earlier.

If S-CSCF just changes the Request URI, then the same mechanism for indicating MRFC parameters is passed through with the INVITE. The S-CSCF would also need to do some mapping between the original Request URI and the new Request URI for the intermediate request messages (e.g. PRACK, COMET/UPDATE) because the AS would still use the original Request URI and the MRFC would need to receive the new Request URI. The ACK and further INVITEs sent from the AS would use the new Request URI that was returned in the Contact header in response to the original INVITE.

Summary

1. Rel-5 should include support for basic call scenarios for tones, announcements, transcoding, and conference calls. This includes a description of how to pass instructions for the requested function using XML within the message body.
2. Rel-5 should include support for the OPTIONS request to return MRFC (and MGCF) capabilities to the AS.

3. Rel-5 should include support for optimising the signalling when tones/announcements are needed for existing session that it is using and MRFP (or MGW), assuming that the same MRFP (or MGW) gets used for playing the tone/announcement.
4. Consideration should be given in Rel-5 for an option of having AS send request using a generic MRFC request URI. However, this may be need to be deferred to Rel-6 to utilize an IETF based solution with Request URI parameters.

Proposal

Agree to the some or all of the concepts described in this paper and use as a reference when considering the CRs for specific changes to 3GPP TS 24.229.

3GPP TSG-CN1 Meeting #24

Tdoc N1-021396
revised N1-021345

Budapest, Hungary, 13. – 17. May 2002

CR-Form-v5

CHANGE REQUEST

⌘ **24.008** **CR** **637** ⌘ **rev** **1** ⌘ Current version: **3.11.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network **X** Core Network ☐

Title:	⌘	Alternative coding of radio access capabilities
Source:	⌘	Siemens AG
Work item code:	⌘	GPRS
Date:	⌘	14.05.02
Category:	⌘	**F**
Release:	⌘	R99

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

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
REL-4 *(Release 4)*
REL-5 *(Release 5)*

Reason for change: ⌘

The MS Radio Access capability IE is included in GMM messages and in RLC/MAC control messages. Due to the introduction of new fields in R99 which are included for each supported band, the overall length of the binary coded IE has significantly increased. If the MS Radio Access Capabilities have to be included in the Packet Resource Request message for RLC/MAC in GPRS mode, there are only **78** bits left for the coding of the MS RA capability value part (for Rel99, Rel-4 and Rel-5). This leads to the problem that maximal two bands could be included.

In order to decrease this length an alternative coding for the indication of the supported bands is proposed.

Furthermore the conditions under which bands must be included in the IE are clarified.

It has been found that there is a number of CS parameters that the CS specific parameters A5bits, HSCSD, ECSD, SMS_VALUE and SM_VALUE included in the MS RAC IE are neither used by the BSS nor by the SGSN. In the current specification, it is not obvious that the MS is allowed to exclude those parameters. If these parameters are excluded, it will be possible to report more bands to the network.

Summary of change: ⌘

A new list of Additional access technologies struct is introduced. It contains just those capabilities which are different from Access technology to Access Technology. This structure contains always the Access Technology Type, the GMSK Power Capability and the 8PSK Power Capability.

It is proposed to define that the MS is allowed to exclude the CS parameters: A5bits, HSCSD, ECSD, SMS_VALUE and SM_VALUE.

Consequences if not approved:	⌘	In GPRS the MS will from R99 onwards be able to include in maximum two of its supported bands during the TBF establishment and in consequence the network can't assign certain radio resources even the MS would support these.

Clauses affected:	⌘	10.5.5.12a		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

10.5.5.12a MS Radio Access capability

The purpose of the *MS RA capability* information element is to provide the radio part of the network with information concerning radio aspects of the mobile station. The contents might affect the manner in which the network handles the operation of the mobile station.

The *MS RA capability* is a type 4 information element, ~~,~~ with a maximum length of 52 octets.

The value part of a *MS RA capability* information element is coded a shown table 10.5.146/3GPP TS 24.008.

~~– SEMANTIC RULE : Among the three Access Type Technologies GSM 900-P, GSM 900-E and GSM 900-R only one shall be present.~~

~~– The MS shall indicate supported Access Technology Types. e.g. [450, 480, 900, 1800, UMTS] or [850, 1900] MHz bands during a single MM procedure.~~

For the indication of the Access Technology Types the following conditions shall apply:

- Among the three Access Technology Types GSM 900-P, GSM 900-E and GSM 900-R only one shall be present.
- Due to shared radio frequency channel numbers between GSM 1800 and GSM 1900, the mobile station should provide the relevant radio access capability for either GSM 1800 band OR GSM 1900 band, not both.
- The MS shall indicate its supported Access Technology Types during a single MM procedure.
- If the alternative coding by using the Additional access technologies struct is chosen by the mobile station, the mobile station shall indicate its radio access capability for the serving BCCH frequency band in the first included Access capabilities struct.
- The first Access Technology Type shall not be set to "1111".

For error handling the following shall apply:

– ~~Error handling :~~ If a received Access Technology Type is unknown to the receiver, it shall ignore all the corresponding fields;

– If within a known Access Technology Type a receiver recognizes an unknown field it shall ignore it.

– ~~See~~ For more details about error handling of MS radio access capability ~~in~~ see 3GPP TS GSM 08.18.

~~– Due to shared radio frequency channel numbers between 1800 and 1900, the mobile should provide the relevant MS Radio Access capability for either 1800 band OR 1900 band, not both.~~

NOTE: The MS should not add spare bits following the <Content> field for the Access capabilities of an Access Technology Type, i.e. the MS should encode the <Length> field of the < Access capabilities struct > as the length in bits of <Content> only.

Table 10.5.146/3GPP TS 24.008 : *Mobile Station Radio Access Capability* Information Element

< MS Radio Access capability IE > ::=
<**MS Radio Access capability IEI** : 00100100 >
<**Length of MS RA capability**: <octet>> -- *length in octets of MS RA capability value part and spare bits*
<**MS RA capability value part** : < MS RA capability value part struct >>
<spare bits>**; -- *may be used for future enhancements*

<MS RA capability value part struct >::= --*recursive structure allows any number of Access technologies*
{ { < **Access Technology Type**: bit (4) exclude 1111 >
< **Access capabilities** : <Access capabilities struct> > }

| { < **Access Technology Type**: bit (4) == 1111 > -- *structure adding Access technologies with same capabilities*
< **Length** : bit (7) > -- *length in bits of list of Additional access technologies and spare bits*
{ 1 < **Additional access technologies**: < Additional access technologies struct > > } ** 0
<spare bits>** } }

{ 0 | 1 <MS RA capability value part struct> } ;

< Additional access technologies struct > ::=
< **Access Technology Type** : bit (4) >
< **GMSK Power Class** : bit (3) >
< **8PSK Power Class** : bit (2) > ;

< Access capabilities struct > ::=
< **Length** : bit (7) > -- length in bits of Content and spare bits
<Access capabilities : <Content>>
<spare bits>** ; -- expands to the indicated length
-- may be used for future enhancements

< Content > ::=
< **RF Power Capability** : bit (3) >
{ 0 | 1 <**A5 bits** : <A5 bits> > } -- *zero means that the same values apply for parameters as in the immediately preceeding Access capabilities field within this IE*
~~-- *The presence of the A5 bits is mandatory in the 1st Access capabilities struct within this IE.*~~
< **ES IND** : bit >
< **PS** : bit >
< **VGCS** : bit >
< **VBS** : bit >
{ 0 | 1 < **Multislot capability** : Multislot capability struct > } -- *zero means that the same values for multislot parameters as given in an earlier Access capabilities field within this IE apply also here*
-- *Additions in release 99*
{ 0 | 1 < **8PSK Power Capability** : bit(2) >} -- *'1' also means 8PSK modulation capability in uplink.*
< **COMPACT Interference Measurement Capability : bit >**
< **Revision Level Indicator** : bit >
< **UMTS FDD Radio Access Technology Capability** : bit > -- *3G RAT*
< **UMTS 3.84 Mcps TDD Radio Access Technology Capability** : bit > -- *3G RAT*
< **CDMA 2000 Radio Access Technology Capability** : bit >; -- *3G RAT*
error: struct too short, assume features do not exist
-- error: struct too long, ignore data and jump to next Access technology

Table 10.5.146/3GPP TS 24.008 (continued): *Mobile Station Radio Access Capability* IE

< Multislot capability struct > ::=
{ 0 | 1 < **HSCSD multislot class** : bit (5) > }
{ 0 | 1 < **GPRS multislot class** : bit (5) > < **GPRS Extended Dynamic Allocation Capability** : bit > }
{ 0 | 1 < **SMS_VALUE** : bit (4) > < **SM_VALUE** : bit (4) > }
-- *Additions in release 99*
{ 0 | 1 < **ECSD multislot class** : bit (5) > }
{ 0 | 1 < **EGPRS multislot class** : bit (5) > < **EGPRS Extended Dynamic Allocation Capability** : bit > }
{ 0 | 1 < **DTM GPRS Multi Slot Sub-Class**: bit(2)>
<MAC Mode Support : bit>
{0 | 1 <**DTM EGPRS Multi Slot Sub-Class** : bit(2)> } } ;
-- error: struct too short, assume features do not exist

<A5 bits> ::= < A5/1 : bit> <A5/2 : bit> <A5/3 : bit> <A5/4 : bit> <A5/5 : bit> <A5/6 : bit> <A5/7 : bit>; -- bits for circuit mode ciphering algorithms. These fields are not used by the network and may be excluded by the MS.

Access Technology Type
This field indicates the access technology type to be associated with the following access capabilities.

Bits
4 3 2 1
0 0 0 0 GSM P
0 0 0 1 GSM E *--note that GSM E covers GSM P*
0 0 1 0 GSM R *--note that GSM R covers GSM E and GSM P*
0 0 1 1 GSM 1800
0 1 0 0 GSM 1900
0 1 0 1 GSM 450
0 1 1 0 GSM 480
0 1 1 1 GSM 850
1 1 1 1 Indicates the presence of a list of Additional access technologies
All other values are treated as unknown by the receiver.

RF Power Capability, GMSK Power Class (3 bit field)
This field ~~is coded as radio capability in Classmark 3 for the indicated band: it~~ contains the binary coding of ~~he~~ the power class used for GMSK associated with the indicated Access Technology Type (see 3GPP TS 05.05).~~(see GSM 05.05 paragraph 4.1 output power and paragraph 4.1.1 Mobile Station).~~

8PSK Power Capability (2 bit field)
If 8-PSK modulation is supported for uplink, this field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 05.05):
Bits 2 1
0 0 Reserved
0 1 Power class E1
1 0 Power class E2
1 1 Power class E3

8PSK Power Class (2 bit field)
This field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 05.05):
Bits 2 1
0 0 8PSK modulation not supported for uplink
0 1 Power class E1
1 0 Power class E2
1 1 Power class E3

Additional access technologies struct
This structure contains the GMSK Power Class and 8PSK Power Class for an additional Access Technology. All other capabilities for this indicated Access Technology are the same as the capabilities indicated by the preceding Access capabilities struct.

A5/1
0 encryption algorithm A5/1 not available
1 encryption algorithm A5/1 available
A5/2
0 encryption algorithm A5/2 not available
1 encryption algorithm A5/2 available

A5/3
0 encryption algorithm A5/3 not available
1 encryption algorithm A5/3 available
A5/4
0 encryption algorithm A5/4 not available
1 encryption algorithm A5/4 available
A5/5
0 encryption algorithm A5/5 not available
1 encryption algorithm A5/5 available
A5/6
0 encryption algorithm A5/6 not available
1 encryption algorithm A5/6 available
A5/7
0 encryption algorithm A5/7 not available
1 encryption algorithm A5/7 available

ES IND – (Controlled early Classmark Sending)
0 "controlled early Classmark Sending" option is not implemented
1 "controlled early Classmark Sending" option is implemented

Table 10.5.146/3GPP TS 24.008 (concluded): *Mobile Station Radio Access Capability* Information Element

PS – (Pseudo Synchronisation)
0 PS capability not present
1 PS capability present

VGCS – (Voice Group Call Service)
0 no VGCS capability or no notifications wanted
1 VGCS capability and notifications wanted.

VBS – (Voice Broadcast Service)
0 no VBS capability or no notifications wanted
1 VBS capability and notifications wanted

HSCSD Multi Slot Class
The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS GSM 05.02. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

GPRS Multi Slot Class
The GPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS GSM 05.02.

ECSD Multi Slot Class
The presence of this field indicates ECSD capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS GSM 05.02. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

EGPRS Multi Slot Class
The presence of this field indicates EGPRS capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The EGPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS GSM 05.02.

GPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for GPRS is not implemented
1 Extended Dynamic Allocation Capability for GPRS is implemented
EGPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for EGPRS is not implemented
1 Extended Dynamic Allocation Capability for EGPRS is implemented

SMS_VALUE (Switch-Measure-Switch) (4 bit field)
The SMS field indicates the time needed for the mobile station to switch from one radio channel to another, perform a neighbour cell power measurement, and the switch from that radio channel to another radio channel. This field is

not used by the network and may be excluded by the MS.
Bits
4 3 2 1
0 0 0 0 1/4 timeslot (~144 microseconds)
0 0 0 1 2/4 timeslot (~288 microseconds)
0 0 1 0 3/4 timeslot (~433 microseconds)
. . .
1 1 1 1 16/4 timeslot (~2307 microseconds)
(SM_VALUE) Switch-Measure (4 bit field)
The SM field indicates the time needed for the mobile station to switch from one radio channel to another and perform a neighbour cell power measurement. This field is not used by the network and may be excluded by the MS.
Bits
4 3 2 1
0 0 0 0 1/4 timeslot (~144 microseconds)
0 0 0 1 2/4 timeslot (~288 microseconds)
0 0 1 0 3/4 timeslot (~433 microseconds)
. . .
1 1 1 1 16/4 timeslot (~2307 microseconds)

DTM GPRS Multi Slot Sub-Class (2 bit field)
~~**DTM GPRS Multi Slot Sub-Class (2 bit field)**~~
This field indicates the GPRS DTM capabilities of the MS. The GPRS DTM Multi Slot Sub-Class is independent from the Multi Slot Capabilities field.
Bits
2 1
0 0 Sub-Class 1 supported
0 1 Sub-Class 5 supported
1 0 Sub-Class 9 supported
1 1 Reserved for future extension. ~~-~~If received, the network shall interpret this as '00'.

DTM EGPRS Multi Slot Sub-Class (2 bit field)
~~**DTM EGPRS Multi Slot Sub-Class (2 bit field)**~~
This field indicates the EGPRS DTM capabilities of the MS. ~~-~~The DTM EGPRS Multi Slot Sub-Class is independent from the Multi Slot Capabilities field. This field shall be included only if the mobile station supports EGPRS DTM. This field is coded as the DTM GPRS Multislot Sub-Class field.

MAC Mode Support (1 bit field)
~~MAC Mode Support (1 bit field)~~
This field indicates whether the MS supports Dynamic and Fixed Allocation or only supports Exclusive Allocation.
Bit~~s~~
~~1~~
0 Dynamic and Fixed Allocation not supported
1 Dynamic and Fixed allocation supported

COMPACT Interference Measurement Capability (1 bit field)
~~COMPACT Interference Measurement Capability~~
Bit
0 COMPACT Interference Measurement Capability is not implemented
1 COMPACT Interference Measurement Capability is implemented
~~0 COMPACT Interference Measurement Capability is not implemented~~
~~1 COMPACT Interference Measurement Capability is implemented~~

Revision Level Indicator (1 bit field)
Bit
0 The ME is Release '98 or older
1 The ME is Release '99 onwards

UMTS FDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS FDD not supported
1 UMTS FDD supported

UMTS 3.84 Mcps TDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS **3.84 Mcps** TDD not supported
1 UMTS **3.84 Mcps** TDD supported

CDMA 2000 Radio Access Technology Capability (1 bit field)
Bit
0 CDMA2000 not supported
1 CDMA2000 supported

3GPP TSG-CN1 Meeting #24

Tdoc N1-021397
revised N1-021346

Budapest, Hungary, 13. – 17. May 2002

CR-Form-v5

CHANGE REQUEST

⌘ **24.008** **CR** **638** ⌘ **rev** **1** ⌘ Current version: **4.6.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network **X** Core Network ☐

Title:	⌘	Alternative coding of radio access capabilities			
Source:	⌘	Siemens AG			
Work item code:	⌘	GPRS	***Date:*** ⌘	14.05.02	
Category:	⌘	**A**	***Release:*** ⌘	REL-4	
		Use one of the following categories:		*Use one of the following releases:*	
		F *(correction)*		*2*	*(GSM Phase 2)*
		A *(corresponds to a correction in an earlier release)*		*R96*	*(Release 1996)*
		B *(addition of feature),*		*R97*	*(Release 1997)*
		C *(functional modification of feature)*		*R98*	*(Release 1998)*
		D *(editorial modification)*		*R99*	*(Release 1999)*
		Detailed explanations of the above categories can be found in 3GPP TR 21.900.		*REL-4*	*(Release 4)*
				REL-5	*(Release 5)*

Reason for change:	⌘	The MS Radio Access capability IE is included in GMM messages and in RLC/MAC control messages. Due to the introduction of new fields in R99 which are included for each supported band, the overall length of the binary coded IE has significantly increased. If the MS Radio Access Capabilities have to be included in the Packet Resource Request message for RLC/MAC in GPRS mode, there are only **78** bits left for the coding of the MS RA capability value part (for Rel99, Rel-4 and Rel-5). This leads to the problem that maximal two bands could be included. In order to decrease this length an alternative coding for the indication of the supported bands is proposed. Furthermore the conditions under which bands must be included in the IE are clarified. It has been found that there is a number of CS parameters that the CS specific parameters A5bits, HSCSD, ECSD, SMS_VALUE and SM_VALUE included in the MS RAC IE are neither used by the BSS nor by the SGSN. In the current specification, it is not obvious that the MS is allowed to exclude those parameters. If these parameters are excluded, it will be possible to report more bands to the network.
Summary of change:	⌘	A new list of Additional access technologies struct is introduced. It contains just those capabilities which are different from Access technology to Access Technology. This structure contains always the Access Technology Type, the GMSK Power Capability and the 8PSK Power Capability. It is proposed to define that the MS is allowed to exclude the CS parameters: A5bits, HSCSD, ECSD, SMS_VALUE and SM_VALUE.

Consequences if not approved:	⌘	In GPRS the MS will from R99 onwards be able to include in maximum two of its supported bands during the TBF establishment and in consequence the network can't assign certain radio resources even the MS would support these.

Clauses affected:	⌘	10.5.5.12a		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

10.5.5.12a MS Radio Access capability

The purpose of the *MS RA capability* information element is to provide the radio part of the network with information concerning radio aspects of the mobile station. The contents might affect the manner in which the network handles the operation of the mobile station.

The *MS RA capability* is a type 4 information element, with a maximum length of 52 octets.

The value part of a *MS RA capability* information element is coded a shown table 10.5.146/3GPP TS 24.008.

~~– SEMANTIC RULE: Among the three Access Type Technologies GSM 900-P, GSM 900-E and GSM 900-R only one shall be present.~~

~~– The MS shall indicate supported Access Technology Types. e.g. [450, 480, 900, 1800, UMTS] or [700, 850, 1900] MHz bands during a single MM procedure.~~

For the indication of the Access Technology Types the following conditions shall apply:

- Among the three Access Type Technologies GSM 900-P, GSM 900-E and GSM 900-R only one shall be present.
- Due to shared radio frequency channel numbers between GSM 1800 and GSM 1900, the mobile station should provide the relevant radio access capability for either GSM 1800 band OR GSM 1900 band, not both.
- The MS shall indicate its supported Access Technology Types during a single MM procedure.
- If the alternative coding by using the Additional access technologies struct is chosen by the mobile station, the mobile station shall indicate its radio access capability for the serving BCCH frequency band in the first included Access capabilities struct.
- The first Access Technology Type shall not be set to "1111".

For error handling the following shall apply:

– ~~Error handling:~~ If a received Access Technology Type is unknown to the receiver, it shall ignore all the corresponding fields.

– If within a known Access Technology Type a receiver recognizes an unknown field it shall ignore it.

– ~~See~~ For more details about error handling of MS radio access capability ~~in~~ see 3GPP TS 48.018 [86].

~~– Due to shared radio frequency channel numbers between 1800 and 1900, the mobile should provide the relevant MS Radio Access capability for either 1800 band OR 1900 band, not both.~~

Table 10.5.146/3GPP TS 24.008: *Mobile Station Radio Access Capability* Information Element

< MS Radio Access capability IE > ::=
<**MS Radio Access capability IEI** : 00100100 >
<**Length of MS RA capability**: <octet>> -- *length in octets of MS RA capability value part and spare bits*
<**MS RA capability value part** : < MS RA capability value part struct >>
<spare bits>**; -- *may be used for future enhancements*

<MS RA capability value part struct >::= --*recursive structure allows any number of Access technologies*
{ { < **Access Technology Type**: bit (4) exclude 1111 >
< **Access capabilities** : <Access capabilities struct> > }

| { < **Access Technology Type**: bit (4) == 1111 > -- *structure adding Access technologies with same capabilities*
< **Length** : bit (7) > -- *length in bits of list of Additional access technologies and spare bits*
{ 1 < **Additional access technologies**: < Additional access technologies struct > > } ** 0
<spare bits>** } }

{ 0 | 1 <MS RA capability value part struct> } ;

< Additional access technologies struct > ::=
< **Access Technology Type** : bit (4) >
< **GMSK Power Class** : bit (3) >
< **8PSK Power Class** : bit (2) > ;

< Access capabilities struct > ::=
< **Length** : bit (7) > -- length in bits of Content and spare bits
<Access capabilities : <Content>>
<spare bits>** ; -- expands to the indicated length
-- may be used for future enhancements

< Content > ::=
< **RF Power Capability** : bit (3) >
{ 0 | 1 <**A5 bits** : <A5 bits> > } -- *zero means that the same values apply for parameters as in the immediately preceeding Access capabilities field within this IE*
~~-- *The presence of the A5 bits is mandatory in the 1st Access capabilities struct within this IE.*~~
< **ES IND** : bit >
< **PS** : bit >
< **VGCS** : bit >
< **VBS** : bit >
{ 0 | 1 < **Multislot capability** : Multislot capability struct > } -- *zero means that the same values for multislot parameters as given in an earlier Access capabilities field within this IE apply also here*
-- Additions in release 99
{ 0 | 1 < **8PSK Power Capability** : bit(2) >} -- *'1' also means 8PSK modulation capability in uplink.*
< **COMPACT Interference Measurement Capability : bit >**
< **Revision Level Indicator** : bit >
< **UMTS FDD Radio Access Technology Capability** : bit > —-- *3G RAT*
< **UMTS 3.84 Mcps TDD Radio Access Technology Capability** : bit > —-- *3G RAT*
< **CDMA 2000 Radio Access Technology Capability** : bit > —-- *3G RAT*
-- Additions in release 4
< **UMTS 1.28 Mcps TDD Radio Access Technology Capability**: bit >—-- *3G RAT*
~~*-- Additions in release 4*~~
< GERAN Feature Package 1 : bit >
{ 0 | 1 < **Extended DTM GPRS Multi Slot Class** : bit(2) >
< **Extended DTM EGPRS Multi Slot Class** : bit(2) > };
-- error: struct too short, assume features do not exist
-- error: struct too long, ignore data and jump to next Access technology

Table 10.5.146/3GPP TS 24.008 (continued): *Mobile Station Radio Access Capability* IE

< Multislot capability struct > ::=
{ 0 | 1 < **HSCSD multislot class** : bit (5) > }
{ 0 | 1 < **GPRS multislot class** : bit (5) > < **GPRS Extended Dynamic Allocation Capability** : bit > }
{ 0 | 1 < **SMS_VALUE** : bit (4) > < **SM_VALUE** : bit (4) > }
-- *Additions in release 99*
{ 0 | 1 < **ECSD multislot class** : bit (5) > }
{ 0 | 1 < **EGPRS multislot class** : bit (5) > < **EGPRS Extended Dynamic Allocation Capability** : bit > }
{0 | 1 < **DTM GPRS Multi Slot Class**: bit(2)>
<MAC Mode Support : bit>
{0 | 1 <**EGPRS DTM Multi Slot Class** : bit(2)> } } ;
-- error: struct too short, assume features do not exist

<A5 bits> ::= < A5/1 : bit> <A5/2 : bit> <A5/3 : bit> <A5/4 : bit> <A5/5 : bit> <A5/6 : bit> <A5/7 : bit>; -- bits for circuit mode ciphering algorithms. These fields are not used by the network and may be excluded by the MS.

Access Technology Type
This field indicates the access technology type to be associated with the following access capabilities.

Bits
4 3 2 1
0 0 0 0 GSM P
0 0 0 1 GSM E --*note that GSM E covers GSM P*
0 0 1 0 GSM R --*note that GSM R covers GSM E and GSM P*
0 0 1 1 GSM 1800
0 1 0 0 GSM 1900
0 1 0 1 GSM 450
0 1 1 0 GSM 480
0 1 1 1 GSM 850
1 0 0 0 GSM 700
1 1 1 1 Indicates the presence of a list of Additional access technologies
All other values are treated as unknown by the receiver.

RF Power Capability, GMSK Power Class (3 bit field)
This field ~~is coded as radio capability in Classmark 3 for the indicated band: it~~ contains the binary coding of ~~he~~the power class used for GMSK associated with the indicated Access Technology Type (see 3GPP TS 45.005). ~~(see 3GPP TS 45.005 [33] paragraph 4.1 output power and paragraph 4.1.1 Mobile Station).~~

8PSK Power Capability(2 bit field)
If 8-PSK modulation is supported for uplink, this field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 45.005 [33]):
Bits 2 1
0 0 Reserved
0 1 Power class E1
1 0 Power class E2
1 1 Power class E3

8PSK Power Class (2 bit field)
This field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 05.05):
Bits 2 1
0 0 8PSK modulation not supported for uplink
0 1 Power class E1
1 0 Power class E2
1 1 Power class E3

Additional access technologies struct
This structure contains the GMSK Power Class and 8PSK Power Class for an additional Access Technology. All other capabilities for this indicated Access Technology are the same as the capabilities indicated by the preceding Access capabilities struct.

A5/1
0 encryption algorithm A5/1 not available
1 encryption algorithm A5/1 available
A5/2
0 encryption algorithm A5/2 not available

1 encryption algorithm A5/2 available
A5/3
0 encryption algorithm A5/3 not available
1 encryption algorithm A5/3 available
A5/4
0 encryption algorithm A5/4 not available
1 encryption algorithm A5/4 available
A5/5
0 encryption algorithm A5/5 not available
1 encryption algorithm A5/5 available
A5/6
0 encryption algorithm A5/6 not available
1 encryption algorithm A5/6 available
A5/7
0 encryption algorithm A5/7 not available
1 encryption algorithm A5/7 available

ES IND – (Controlled early Classmark Sending)
0 "controlled early Classmark Sending" option is not implemented
1 "controlled early Classmark Sending" option is implemented

Table 10.5.146/3GPP TS 24.008 (concluded): *Mobile Station Radio Access Capability* Information Element

PS – (Pseudo Synchronisation)
0 PS capability not present
1 PS capability present

VGCS – (Voice Group Call Service)
0 no VGCS capability or no notifications wanted
1 VGCS capability and notifications wanted.

VBS – (Voice Broadcast Service)
0 no VBS capability or no notifications wanted
1 VBS capability and notifications wanted

HSCSD Multi Slot Class
The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32]. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

GPRS Multi Slot Class
The GPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

-- Additions in release 99

ECSD Multi Slot Class
The presence of this field indicates ECSD capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32]. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

EGPRS Multi Slot Class
The presence of this field indicates EGPRS capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The EGPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

GPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for GPRS is not implemented
1 Extended Dynamic Allocation Capability for GPRS is implemented
EGPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for EGPRS is not implemented
1 Extended Dynamic Allocation Capability for EGPRS is implemented

SMS_VALUE (Switch-Measure-Switch) (4 bit field)
The SMS field indicates the time needed for the mobile station to switch from one radio channel to another, perform a neighbour cell power measurement, and the switch from that radio channel to another radio channel. This field is not used by the network and may be excluded by the MS.
Bits
4 3 2 1
0 0 0 0 1/4 timeslot (~144 microseconds)
0 0 0 1 2/4 timeslot (~288 microseconds)
0 0 1 0 3/4 timeslot (~433 microseconds)
. . .
1 1 1 1 16/4 timeslot (~2307 microseconds)
(SM_VALUE) Switch-Measure (4 bit field)
The SM field indicates the time needed for the mobile station to switch from one radio channel to another and perform a neighbour cell power measurement. This field is not used by the network and may be excluded by the MS.
Bits
4 3 2 1
0 0 0 0 1/4 timeslot (~144 microseconds)
0 0 0 1 2/4 timeslot (~288 microseconds)
0 0 1 0 3/4 timeslot (~433 microseconds)
. . .
1 1 1 1 16/4 timeslot (~2307 microseconds)

DTM GPRS Multi Slot Class (2 bit field)
This field indicates the GPRS DTM multislot capabilities of the MS. It is coded as follows:
Bits
2 1
0 0 Multislot class 1 supported
0 1 Multislot class 5 supported
1 0 Multislot class 9 supported
1 1 Reserved for future extension. If received, the network shall interpret this as '00'

MAC Mode Support (1 bit field)
~~MAC Mode Support (1 bit field)~~
This field indicates whether the MS supports Dynamic and Fixed Allocation or only supports Exclusive Allocation
Bits
1
0 Dynamic and Fixed Allocation not supported
1 Dynamic and Fixed allocation supported

EGPRS DTM Multi Slot Class (2 bit field)
This field indicates the EGPRS DTM multislot capabilities of the MS. This field shall be included only if the mobile station supports EGPRS DTM. This field is coded as the DTM GPRS multislot Class field.

COMPACT Interference Measurement Capability (1 bit field)
~~COMPACT Interference Measurement Capability~~
Bit
0 COMPACT Interference Measurement Capability is not implemented
1 COMPACT Interference Measurement Capability is implemented
~~0 COMPACT Interference Measurement Capability is not implemented~~
~~1 COMPACT Interference Measurement Capability is implemented~~

Revision Level Indicator(1 bit field)
Bit
0 The ME is Release '98 or older
1 The ME is Release '99 onwards

UMTS FDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS FDD not supported
1 UMTS FDD supported

UMTS 3.84 Mcps TDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS 3.84 Mcps TDD not supported
1 UMTS 3.84 Mcps TDD supported

CDMA 2000 Radio Access Technology Capability (1 bit field)
Bit
0 CDMA2000 not supported
1 CDMA2000 supported

UMTS 1.28 Mcps TDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS 1.28 Mcps TDD not supported
1 UMTS 1.28 Mcps TDD supported

GERAN Feature Package 1 (1 bit field)
This field indicates whether the MS supports the GERAN Feature Package 1 (see 3GPP TS 44.060). It is coded as follows:

Bit
0 GERAN feature package 1 not supported.
1 GERAN feature package 1 supported.

Extended GPRS DTM Multi Slot Class (2 bit field)
This field indicates the extended GPRS DTM capabilities of the MS and shall be interpreted in conjunction with the GPRS DTM Multi Slot Class field. It is coded as follows, where 'DGMSC' denotes the DTM GPRS multislot class field:

0 0	**0 1**	Multislot class 3 supported

3GPP TSG-CN1 Meeting #24

Tdoc N1-021398
revised N1-021347

Budapest, Hungary, 13. – 17. May 2002

CR-Form-v5

CHANGE REQUEST

⌘ **24.008** **CR** **639** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE **X** Radio Access Network **X** Core Network ☐

Title:	⌘	Alternative coding of radio access capabilities		
Source:	⌘	Siemens AG		
Work item code:	⌘	GPRS	***Date:*** ⌘	14.05.02
Category:	⌘	**A**	***Release:*** ⌘	REL-5

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

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
REL-4 *(Release 4)*
REL-5 *(Release 5)*

Reason for change: ⌘ The MS Radio Access capability IE is included in GMM messages and in RLC/MAC control messages. Due to the introduction of new fields in R99 which are included for each supported band, the overall length of the binary coded IE has significantly increased. If the MS Radio Access Capabilities have to be included in the Packet Resource Request message for RLC/MAC in GPRS mode, there are only **78** bits left for the coding of the MS RA capability value part (for Rel99, Rel-4 and Rel-5). This leads to the problem that maximal two bands could be included.

In order to decrease this length an alternative coding for the indication of the supported bands is proposed.

Furthermore the conditions under which bands must be included in the IE are clarified.

It has been found that there is a number of CS parameters that the CS specific parameters A5bits, HSCSD, ECSD, SMS_VALUE and SM_VALUE included in the MS RAC IE are neither used by the BSS nor by the SGSN. In the current specification, it is not obvious that the MS is allowed to exclude those parameters. If these parameters are excluded, it will be possible to report more bands to the network.

Summary of change: ⌘ A new list of Additional access technologies struct is introduced. It contains just those capabilities which are different from Access technology to Access Technology. This structure contains always the Access Technology Type, the GMSK Power Capability and the 8PSK Power Capability.

It is proposed to define that the MS is allowed to exclude the CS parameters: A5bits, HSCSD, ECSD, SMS_VALUE and SM_VALUE.

Consequences if not approved:	⌘	In GPRS the MS will from R99 onwards be able to include in maximum two of its supported bands during the TBF establishment and in consequence the network can't assign certain radio resources even the MS would support these.

Clauses affected:	⌘	10.5.5.12a		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

10.5.5.12a MS Radio Access capability

The purpose of the *MS RA capability* information element is to provide the radio part of the network with information concerning radio aspects of the mobile station. The contents might affect the manner in which the network handles the operation of the mobile station.

The *MS RA capability* is a type 4 information element, with a maximum length of 52 octets.

The value part of a *MS RA capability* information element is coded a shown table 10.5.146/3GPP TS 24.008.

~~– SEMANTIC RULE: Among the three Access Type Technologies GSM 900-P, GSM 900-E and GSM 900-R only one shall be present.~~

~~– The MS shall indicate supported Access Technology Types. e.g. [450, 480, 900, 1800, UMTS] or [700, 850, 1900] MHz bands during a single MM procedure.~~

For the indication of the Access Technology Types the following conditions shall apply:

- Among the three Access Type Technologies GSM 900-P, GSM 900-E and GSM 900-R only one shall be present.
- Due to shared radio frequency channel numbers between GSM 1800 and GSM 1900, the mobile station should provide the relevant radio access capability for either GSM 1800 band OR GSM 1900 band, not both.
- The MS shall indicate its supported Access Technology Types during a single MM procedure.
- If the alternative coding by using the Additional access technologies struct is chosen by the mobile station, the mobile station shall indicate its radio access capability for the serving BCCH frequency band in the first included Access capabilities struct.
- The first Access Technology Type shall not be set to "1111".

For error handling the following shall apply:

– ~~Error handling:~~ If a received Access Technology Type is unknown to the receiver, it shall ignore all the corresponding fields.

– If within a known Access Technology Type a receiver recognizes an unknown field it shall ignore it.

– ~~See~~ For more details about error handling of MS radio access capability ~~in~~ see3GPP TS 48.018 [86].

~~– Due to shared radio frequency channel numbers between 1800 and 1900, the mobile should provide the relevant MS Radio Access capability for either 1800 band OR 1900 band, not both.~~

Table 10.5.146/3GPP TS 24.008: *Mobile Station Radio Access Capability* Information Element

< MS Radio Access capability IE > ::=
<**MS Radio Access capability IEI** : 00100100 >
<**Length of MS RA capability**: <octet>> -- *length in octets of MS RA capability value part and spare bits*
<**MS RA capability value part** : < MS RA capability value part struct >>
<spare bits>**; -- *may be used for future enhancements*

<MS RA capability value part struct >::= --*recursive structure allows any number of Access technologies*
{ { < **Access Technology Type**: bit (4) exclude 1111 >
< **Access capabilities** : <Access capabilities struct> > }

| { < **Access Technology Type**: bit (4) == 1111 > -- *structure adding Access technologies with same capabilities*
< **Length** : bit (7) > -- *length in bits of list of Additional access technologies and spare bits*
{ 1 < **Additional access technologies**: < Additional access technologies struct > > } ** 0
<spare bits>** } }

{ 0 | 1 <MS RA capability value part struct> } ;

< Additional access technologies struct > ::=
< **Access Technology Type** : bit (4) >
< **GMSK Power Class** : bit (3) >
< **8PSK Power Class** : bit (2) > ;

< Access capabilities struct > ::=
< **Length** : bit (7) > -- length in bits of Content and spare bits
<Access capabilities : <Content>>
<spare bits>** ; -- expands to the indicated length
-- may be used for future enhancements

< Content > ::=
< **RF Power Capability** : bit (3) >
{ 0 | 1 <**A5 bits** : <A5 bits> > } -- *zero means that the same values apply for parameters as in the immediately preceeding Access capabilities field within this IE*
~~-- *The presence of the A5 bits is mandatory in the 1st Access capabilities struct within this IE.*~~
< **ES IND** : bit >
< **PS** : bit >
< **VGCS** : bit >
< **VBS** : bit >
{ 0 | 1 < **Multislot capability** : Multislot capability struct > } -- *zero means that the same values for multislot parameters as given in an earlier Access capabilities field within this IE apply also here*
-- Additions in release 99
{ 0 | 1 < **8PSK Power Capability** : bit(2) >} -- *'1' also means 8PSK modulation capability in uplink.*
< **COMPACT Interference Measurement Capability : bit >**
< **Revision Level Indicator** : bit >
< **UMTS FDD Radio Access Technology Capability** : bit > —-- *3G RAT*
< **UMTS 3.84 Mcps TDD Radio Access Technology Capability** : bit > —-- *3G RAT*
< **CDMA 2000 Radio Access Technology Capability** : bit > —-- *3G RAT*
-- Additions in release 4
< **UMTS 1.28 Mcps TDD Radio Access Technology Capability**: bit > —-- *3G RAT*
~~*-- Additions in release 4*~~
< GERAN Feature Package 1 : bit >
{ 0 | 1 < **Extended DTM GPRS Multi Slot Class** : bit(2) >
< **Extended DTM EGPRS Multi Slot Class** : bit(2) > };
-- error: struct too short, assume features do not exist
-- error: struct too long, ignore data and jump to next Access technology

Table 10.5.146/3GPP TS 24.008 (continued): *Mobile Station Radio Access Capability* IE

< Multislot capability struct > ::=
{ 0 | 1 < **HSCSD multislot class** : bit (5) > }
{ 0 | 1 < **GPRS multislot class** : bit (5) > < **GPRS Extended Dynamic Allocation Capability** : bit > }
{ 0 | 1 < **SMS_VALUE** : bit (4) > < **SM_VALUE** : bit (4) > }
-- *Additions in release 99*
{ 0 | 1 < **ECSD multislot class** : bit (5) > }
{ 0 | 1 < **EGPRS multislot class** : bit (5) > < **EGPRS Extended Dynamic Allocation Capability** : bit > }
{0 | 1 < **DTM GPRS Multi Slot Class**: bit(2)>
<MAC Mode Support : bit>
{0 | 1 <**EGPRS DTM Multi Slot Class** : bit(2)> } } ;
-- error: struct too short, assume features do not exist

<A5 bits> ::= < A5/1 : bit> <A5/2 : bit> <A5/3 : bit> <A5/4 : bit> <A5/5 : bit> <A5/6 : bit> <A5/7 : bit>; -- bits for circuit mode ciphering algorithms. These fields are not used by the network and may be excluded by the MS.

Access Technology Type
This field indicates the access technology type to be associated with the following access capabilities.

Bits
4 3 2 1
0 0 0 0 GSM P
0 0 0 1 GSM E --*note that GSM E covers GSM P*
0 0 1 0 GSM R --*note that GSM R covers GSM E and GSM P*
0 0 1 1 GSM 1800
0 1 0 0 GSM 1900
0 1 0 1 GSM 450
0 1 1 0 GSM 480
0 1 1 1 GSM 850
1 0 0 0 GSM 700
1 1 1 1 Indicates the presence of a list of Additional access technologies
All other values are treated as unknown by the receiver.

RF Power Capability, GMSK Power Class (3 bit field)
This field ~~is coded as radio capability in Classmark 3 for the indicated band: it~~ contains the binary coding of ~~he~~ the power class used for GMSK associated with the indicated Access Technology Type (see 3GPP TS 45.005). ~~(see 3GPP TS 45.005 [33] paragraph 4.1 output power and paragraph 4.1.1 Mobile Station).~~

8PSK Power Capability (2 bit field)
If 8-PSK modulation is supported for uplink, this field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 45.005 [33]):
Bits 2 1
0 0 Reserved
0 1 Power class E1
1 0 Power class E2
1 1 Power class E3

8PSK Power Class (2 bit field)
This field indicates the radio capability for 8-PSK modulation. The following coding is used (see 3GPP TS 05.05):
Bits 2 1
0 0 8PSK modulation not supported for uplink
0 1 Power class E1
1 0 Power class E2
1 1 Power class E3

Additional access technologies struct
This structure contains the GMSK Power Class and 8PSK Power Class for an additional Access Technology. All other capabilities for this indicated Access Technology are the same as the capabilities indicated by the preceding Access capabilities struct.

A5/1
0 encryption algorithm A5/1 not available
1 encryption algorithm A5/1 available
A5/2
0 encryption algorithm A5/2 not available

1 encryption algorithm A5/2 available
A5/3
0 encryption algorithm A5/3 not available
1 encryption algorithm A5/3 available
A5/4
0 encryption algorithm A5/4 not available
1 encryption algorithm A5/4 available
A5/5
0 encryption algorithm A5/5 not available
1 encryption algorithm A5/5 available
A5/6
0 encryption algorithm A5/6 not available
1 encryption algorithm A5/6 available
A5/7
0 encryption algorithm A5/7 not available
1 encryption algorithm A5/7 available

ES IND – (Controlled early Classmark Sending)
0 "controlled early Classmark Sending" option is not implemented
1 "controlled early Classmark Sending" option is implemented

Table 10.5.146/3GPP TS 24.008 (concluded): *Mobile Station Radio Access Capability* Information Element

PS – (Pseudo Synchronisation)
0 PS capability not present
1 PS capability present

VGCS – (Voice Group Call Service)
0 no VGCS capability or no notifications wanted
1 VGCS capability and notifications wanted.

VBS – (Voice Broadcast Service)
0 no VBS capability or no notifications wanted
1 VBS capability and notifications wanted

HSCSD Multi Slot Class
The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32]. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

GPRS Multi Slot Class
The GPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

-- Additions in release 99

ECSD Multi Slot Class
The presence of this field indicates ECSD capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32]. This field is not used by the network and may be excluded by the MS.
Range 1 to 18, all other values are reserved.

EGPRS Multi Slot Class
The presence of this field indicates EGPRS capability. Whether the MS is capable of 8-PSK modulation in uplink is indicated by the presence of 8-PSK Power Capability field. The EGPRS Multi Slot Class field is coded as the binary representation of the multislot class defined in 3GPP TS 45.002 [32].

GPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for GPRS is not implemented
1 Extended Dynamic Allocation Capability for GPRS is implemented
EGPRS Extended Dynamic Allocation Capability
0 Extended Dynamic Allocation Capability for EGPRS is not implemented
1 Extended Dynamic Allocation Capability for EGPRS is implemented

SMS_VALUE (Switch-Measure-Switch) (4 bit field)
The SMS field indicates the time needed for the mobile station to switch from one radio channel to another, perform a neighbor cell power measurement, and the switch from that radio channel to another radio channel. This field is not used by the network and may be excluded by the MS.
Bits
4 3 2 1
0 0 0 0 1/4 timeslot (~144 microseconds)
0 0 0 1 2/4 timeslot (~288 microseconds)
0 0 1 0 3/4 timeslot (~433 microseconds)
. . .
1 1 1 1 16/4 timeslot (~2307 microseconds)
(SM_VALUE) Switch-Measure (4 bit field)
The SM field indicates the time needed for the mobile station to switch from one radio channel to another and perform a neighbour cell power measurement. This field is not used by the network and may be excluded by the MS.
Bits
4 3 2 1
0 0 0 0 1/4 timeslot (~144 microseconds)
0 0 0 1 2/4 timeslot (~288 microseconds)
0 0 1 0 3/4 timeslot (~433 microseconds)
. . .
1 1 1 1 16/4 timeslot (~2307 microseconds)

DTM GPRS Multi Slot Class (2 bit field)
This field indicates the GPRS DTM multislot capabilities of the MS. It is coded as follows:
Bits
2 1
0 0 Multislot class 1 supported
0 1 Multislot class 5 supported
1 0 Multislot class 9 supported
1 1 Reserved for future extension. If received, the network shall interpret this as '00'

MAC Mode Support (1 bit field)~~MAC Mode Support (1 bit field)~~
This field indicates whether the MS supports Dynamic and Fixed Allocation or only supports Exclusive Allocation
Bit~~s~~
~~1~~
0 Dynamic and Fixed Allocation not supported
1 Dynamic and Fixed allocation supported

EGPRS DTM Multi Slot Class (2 bit field)
This field indicates the EGPRS DTM multislot capabilities of the MS. This field shall be included only if the mobile station supports EGPRS DTM. This field is coded as the DTM GPRS multislot Class field.

COMPACT Interference Measurement Capability (1 bit field)
~~COMPACT Interference Measurement Capability~~
0 COMPACT Interference Measurement Capability is not implemented
1 COMPACT Interference Measurement Capability is implemented
~~0 COMPACT Interference Measurement Capability is not implemented~~
~~1 COMPACT Interference Measurement Capability is implemented~~

Revision Level Indicator(1 bit field)
Bit
0 The ME is Release '98 or older
1 The ME is Release '99 onwards

UMTS FDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS FDD not supported
1 UMTS FDD supported

UMTS 3.84 Mcps TDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS 3.84 Mcps TDD not supported
1 UMTS 3.84 Mcps TDD supported

CDMA 2000 Radio Access Technology Capability (1 bit field)
Bit
0 CDMA2000 not supported
1 CDMA2000 supported

UMTS 1.28 Mcps TDD Radio Access Technology Capability (1 bit field)
Bit
0 UMTS 1.28 Mcps TDD not supported
1 UMTS 1.28 Mcps TDD supported

GERAN Feature Package 1 (1 bit field)
This field indicates whether the MS supports the GERAN Feature Package 1 (see 3GPP TS 44.060). It is coded as follows:

0 GERAN feature package 1 not supported.
1 GERAN feature package 1 supported.

Extended GPRS DTM Multi Slot Class (2 bit field)
This field indicates the extended GPRS DTM capabilities of the MS and shall be interpreted in conjunction with the GPRS DTM Multi Slot Class field. It is coded as follows, where 'DGMSC' denotes the DTM GPRS multislot class field:

0 1	**0 0**	Multislot class 5 supported	