3GPP TSG CN Plenary, Meeting #11 **Tdoc NP-010065**
Palm Springs, USA. 14th - 16th March 2001

Source: **TSG_CN WG4**

Title: **All LSs sent from CN4 since TSG CN#10**

Agenda item: **6.4.1**

Document for: **Information**

Introduction:

The following LS has been sent by CN4 since the last CN Plenary.
It is forwarded to TSG CN Plenary meeting #11 for information only.

TDOC N4-00xxxx	Subject	To	Cc	Attachment	Sent
N4-010160	LS for clarification of MPTY issues	S1, G4		N4-010096, N4-010097	22nd Jan
N4-010180	LS on proposed fix for GPRS Roaming issues	S2		N4-010091, N4-010092 N4-010093	22nd Jan
N4-010203	Response to SA3 on SA3 agreements on MAPSec	S3			22nd Jan
N4-010204	LS on Maximum size of LCS clients	S1, S2			22nd Jan
N4-010282	LS response on GTP-U version negotiation	R3			16th Feb
N4-010283	LS for "Reply on Default Configurations for Handover"	S4, R2, TSG-T, TSG-Geran, R1	N1		16th Feb
N4-010284	LS highlighting requirements to RAN WG3 for SRNS Relocation with TrFO	R3	S2, N1	N4-001099	16th Feb
N4-010285	LS response on Enhancement of LCS functionality in Rel-4	S2	S1		16th Feb
N4-010291	LS reply to SA3 on request for information to complete security work items	S3			16th Feb
N4-010302	Response to SA1 LS (Tdoc S1-010219) on maximum number of LCS clients in the "privacy client list"	S1, S2			16th Feb
N4-010307	LS Response Lawful Intercept support on the Mc interface	S3			16th Feb
N4-010439	LS on handling of an error case for authentication set retrieval	S2		N4-010440, N4-010441, N4-010442	27th Feb
N4-010483	LS on Maximum number of LCS Clients in LCS Rel-4	S1		N4-010462	05th Mar

3GPP TSG_CN_WG4, Meeting #07 **Tdoc N4-010462**
Sophia Antipolis, FRANCE, 26th February - 2nd March 2001

Source: **NTC**

Title: **Calculation for max number of LCS Clients**

Agenda item: **LCS R4**

Document for: **Discussion**

---

1. Introduction

SA1 discussed about the maximum number of LCS Clients by e-mail. SA1 agreed the consensus of the maximum number of LCS Clients. SA1 delegate proposes the text of the CR to indicate "The privacy list shall support a minimum of 20 entries. The maximum number of entries shall be determined by implementation constraints."

This contribution shows the result of calculation for max number of LCS Clients in order to indicate the available LCS Client number.

2. Calculation for max number of LCS Clients

In the last Madrid meeting, the issue for the max number of LCS Clients was discussed but the correct number didn't be calculated. NTC calculated the available max number of LCS Clients based on N4-010375•(CR to 29.002). This contribution referred to N4-010031 for the available MAP length and attached in annex A.

2.1 Total length except ext-externalClientList

InsertSubscriberDataArg	3(1+2)
lcsInformation	3(1+2)
lcs-PrivacyExceptionList	3(1+2)
lcs-PrivacyClass	3(1+2)
ss-Code	3(1+1+1)
ss-Status	7(1+1+5)
notificationToMSUser	3(1+1+1)
externalClientList	163(1+2+(5*32))
plmnClientList	17(1+1+(5*3))
ext-externalClientList	XXX

The total length except ext-externalClientList is 205 octets.

2.2 Maximum guaranteed length of the MAP payload

The maximum guaranteed length is from 3328 octets to 3458 octets by security mode. The contribution uses the 3328 octets.
(See Annex A)

2.3 Available length for ext-externalClientList

The available length for ext-externalClientList is 3123 (3123=3328-205) octets.

2.4 Available LCS Clients

The length for one external client is 32 octets.
If additional 97 LCS Clients are set, 3104(1+2+(97*32)) octets for ext-externalClientList are needed.
If additional 98 LCS Clients are set, 3136(1+2+(98*32)) octets for ext-externalClientList are needed.

ext-externalClientList can set 97 LCS Clients.

3. Conclusion

Additional 97 LCS Clients can set in the lcs-PrivacyClass.

Annex --- the extract of N4-010031

XUDT	BEGIN	with DP	Invoke	no security			3432
				prot. Mode 0			3380
				prot. Mode 1			3350
				prot. Mode 2			3344
			Result	no security			n.a.
				prot. Mode 0			n.a.
				prot. Mode 1			n.a.
				prot. Mode 2			n.a.
		without DP	Invoke	no security			n.a.
				prot. Mode 0			n.a.
				prot. Mode 1			n.a.
				prot. Mode 2			n.a.
			Result	no security			n.a.
				prot. Mode 0			n.a.
				prot. Mode 1			n.a.
				prot. Mode 2			n.a.
	CONTINUE	with DP	Invoke	no security			3414
				prot. Mode 0			3362
				prot. Mode 1			3332
				prot. Mode 2			3328
			Result	no security			3410
				prot. Mode 0			3358
				prot. Mode 1			3328
				prot. Mode 2			3328
		without DP	Invoke	no security			3458
				prot. mode 0			3432
				prot. mode 1			3402
				prot. mode 2			3392
			Result	no security			3454
				prot. mode 0			3428
				prot. mode 1			3398
				prot. mode 2			3392
	END	with DP	Invoke	no security			3420
				prot. mode 0			3368
				prot. mode 1			3338
				prot. mode 2			3328
			Result	no security			3416
				prot. mode 0			3364
				prot. mode 1			3334
				prot. mode 2			3328
		without DP	Invoke	no security			3464
				prot. mode 0			3438
				prot. mode 1			3408
				prot. mode 2			3408
			Result	no security			3460
				prot. mode 0			3434
				prot. mode 1			3404
				prot. mode 2			3392

3GPP TSG-CN WG4 **Tdoc N4-010483**
CN4 Meeting #7, Sophia Antipolis, FRANCE
26th February – 2nd March 2001

Title: **LS on Maximum number of LCS Clients in LCS Rel-4**

Source: **TSG_CN WG4**

To: **TSG_SA1**

Contact Person:

Name: **Miyuki SOEJIMA**
E-mail Address: **miyuki@mob.ntc.co.jp**
Tel. Number: +81 (44) 9007313

---

1. Overall Description:

TSG-CN WG4 have discussed the maximum number of LCS Clients determined by implementation constraints. TSG-CN WG4 concluded that total 102 LCS Clients can be carried by White book SCCP. However considering the future enhancement, privacy extensions and memory capacity, some room should be left for them. Therefore CN4 recommend the total 40 LCS Clients as maximum number for Release 4.

CN4 agreed the CR which defines 40 as the maximum number of LCS Clients.

2. Actions:

To TSG SA1:

ACTION: TSG_CN WG4 asks that TSG SA WG1 to confirm above conclusion of TSG CN WG4.

3. Attachments:

T-doc N4-010462 : Calculation for max number of LCS Clients

4. The next CN4 meeting

The next TSG-CN WG4 meeting is scheduled for 14 – 18 May 2001 in Puerto Rico.

3GPP TSG SA2#15 **S2-001827**
Makuhari, Japan, November 13th – 17th, 2000

3GPP TSG SA2#15 **Tdoc N4-001098**
(Tdoc S2-002062)

Makuhari, Japan, 13th – 17th November, 2000

TITLE: **RE: LS ON SIZE OF RANAP MESSAGES OVER MAP-E**

TO: **TSG-RAN WG3**

TSG-CN WG-4

FROM: **SA2**

CC: **CN WG1, SA WG4**

Contact: Stephen.Terrill@ericsson.com

S2 would like to thank TSG-RAN WG3 for the liaison statement "LS on Size of RANAP messages over MAP-E" (TSGR3#16(00)2914).

The liaison statement contained a number of different approaches as potential solutions to the issue of the signaling transport of the MAP-E interface, and requested S2's view on these issues.

1. On the approach of enhancing the capacity of the MAP-E interface by mandating whitebook SCCP for the MAP-E interface, S2 views that this could be considered as suitable approach for SRNS relocations within the same operators network, and advises that it is not recommended to rely upon whitebook SCCP deployment outside the one operators network before the 1st July 2002.

2. The approach of reducing the size of too large RANAP messages is considered to be a stage 3 issue and not for comment from S2.

3. The approach of introducing an additional layer for segmentation and re-assembly is not recommended.

4. The approach of avoiding the MAP-E interface would introduce and architectural change which was considered as too late for R99.

3GPP TSG SA2#15 **S2-001827**
Makuhari, Japan, November 13th – 17th, 2000

3GPP TSG SA2#15 **Tdoc N4-001099**
(Tdoc S2-002000)

Makuhari, Japan, 13th – 17th November, 2000

TITLE: **RE: LS, SRNS RELOCATION BASED ON GLOBAL TITLE**

TO: **CN4**

CC: **RAN3**

FROM: **SA2**

CC: **CN WG1, SA WG4**

Contact: Stephen.Terrill@ericsson.com

S2 would like to thank N4 for the liaison statement SRNS relocation based on global title (N4-000741).

S2 would like to inform N4 that S2 has concluded the discussion related to SRNS relocation based on global title, and would like to inform that the following has been agreed in S2 for Release 4.

X.y.z UMTS to UMTS handover for circuit switched services

For UMTS to UMTS Inter-MSC Hand-Over / SRNS relocation the MAP E interface transporting RANAP messages shall be used. Alternatively, in the case of intra-PLMN handover, the SRNS reloacation between two MSC-areas may be executed as intra-MSC SRNS relocation. In such a case this will be performed by utilising a direct SCCP connection between the target RNC located in the target MSC-area and the MSC server already involved in the call.

3GPP TSG-CN4 Meeting #06 **Tdoc N4-010091**
BEIJING, CHINA 15th 19th January 2001

CR-Form-v3

CHANGE REQUEST

⌘ **03.60** **CR** ⌘ rev **-** ⌘ Current version: **6.7.0** ⌘

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

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

Title:	⌘	Failure of Update GPRS Location when HLR is not reachable
Source:	⌘	Vodafone UK Ltd
Work item code:	⌘	GPRS R97 ***Date:*** ⌘ 5 Jan 2001
Category:	⌘	**F** (critical correction) ***Release:*** ⌘ R97

Use one of the following categories:
F *(essential 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:	⌘	Returning "Roaming Not Allowed" if the HLR is not reachable can cause undesirable behaviour of the MS which tries to register in an SGSN when a GPRS roaming agreement has not been set up between the HPLMN and VPLMN operators
Summary of change:	⌘	Show the handling of the error "Unknown HLR"
Consequences if not approved:	⌘	Unnecessary denial of CS service to GPRS capable MSs

Clauses affected:	⌘	6.9.1.2.2; 6.9.1.3.2		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	GSM 09.02
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.9.1.2.2 Inter SGSN Routeing Area Update

...

In the case of a rejected routeing area update operation, due to regional subscription or roaming restrictions, or because the SGSN cannot determine the HLR address to establish the GPRS location~~ng~~ update~~ing~~ dialogue, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

...

**** Next modified section ****

6.9.1.3.2 Combined Inter SGSN RA / LA Update

...

In the case of a rejected routeing area update operation, due to regional subscription or roaming restrictions, or because the SGSN cannot determine the HLR address to establish the locating updating dialogue, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

...

3GPP TSG-CN4 Meeting #06 **Tdoc N4-010092**
BEIJING, CHINA 15th 19th January 2001

CR-Form-v3

CHANGE REQUEST

⌘ **03.60** **CR** ⌘ rev **-** ⌘ Current version: **7.5.0** ⌘

*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:	⌘	Failure of Update GPRS Location when HLR is not reachable
Source:	⌘	Vodafone UK Ltd
Work item code:	⌘	GPRS R97
Date:	⌘	5 Jan 2001
Category:	⌘	**A**
Release:	⌘	R98

Use one of the following categories:
F *(essential 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:	⌘	Returning "Roaming Not Allowed" if the HLR is not reachable can cause undesirable behaviour of the MS which tries to register in an SGSN when a GPRS roaming agreement has not been set up between the HPLMN and VPLMN operators
Summary of change:	⌘	Show the handling of the error "Unknown HLR"
Consequences if not approved:	⌘	Unnecessary denial of CS service to GPRS capable MSs

Clauses affected:	⌘	6.9.1.2.2; 6.9.1.3.2		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	GSM 09.02
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.9.1.2.2 Inter SGSN Routeing Area Update

...

In the case of a rejected routeing area update operation, due to regional subscription or roaming restrictions, or because the SGSN cannot determine the HLR address to establish the locating updating dialogue, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

...

**** Next modified section ****

6.9.1.3.2 Combined Inter SGSN RA / LA Update

...

In the case of a rejected routeing area update operation, due to regional subscription or roaming restrictions, or because the SGSN cannot determine the HLR address to establish the locating updating dialogue, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

...

3GPP TSG-CN4 Meeting #06 **Tdoc N4-010093**
BEIJING, CHINA 15th 19th January 2001

CR-Form-v3

CHANGE REQUEST

⌘ **23.060** **CR** ⌘ rev **-** ⌘ Current version: **3.6.0** ⌘

*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:	⌘	Failure of Update GPRS Location when HLR is not reachable
Source:	⌘	Vodafone UK Ltd
Work item code:	⌘	GPRS R97
Date:	⌘	5 Jan 2001
Category:	⌘	**A**
Release:	⌘	R99

Use one of the following categories:
F *(essential 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:	⌘	Returning "Roaming Not Allowed" if the HLR is not reachable can cause undesirable behaviour of the MS which tries to register in an SGSN when a GPRS roaming agreement has not been set up between the HPLMN and VPLMN operators
Summary of change:	⌘	Show the handling of the error "Unknown HLR"
Consequences if not approved:	⌘	Unnecessary denial of CS service to GPRS capable MSs

Clauses affected:	⌘	6.9.1.2.2; 6.9.1.3.2		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	GSM 09.02
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.9.1.2.2 Inter SGSN Routeing Area Update

...

In the case of a rejected routeing area update operation, due to regional subscription or roaming restrictions, or because the SGSN cannot determine the HLR address to establish the locating updating dialogue, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

...

**** Next modified section ****

6.9.1.3.2 Combined Inter SGSN RA / LA Update

...

In the case of a rejected routeing area update operation, due to regional subscription or roaming restrictions, or because the SGSN cannot determine the HLR address to establish the locating updating dialogue, the new SGSN shall not construct an MM context. A reject shall be returned to the MS with an appropriate cause. The MS shall not re-attempt a routeing area update to that RA. The RAI value shall be deleted when the MS is powered-up.

...

3GPP TSG-GERAN WG4 **N4-010096**
Sophia Antipolis, France **(G4-000317)**
20-24 November 2000

Liaison Statement

From: 3GPP TSG GERAN-WG4

To: 3GPP TSG N-WG4

Cc: 3GPP TSG S-WG1

Subject: Request for clarification on disconnecting Multiparty calls when a single call is active.

TSG GERAN WG4 seeks advice from TSG N-WG4 on the following issue.

GSM 04.84 (Phase 2 onwards) clause 1.4.1.2 for managing a single call and a MultiParty call states that:

"Disconnect the MPTY

This is achieved by the same procedure as disconnecting a held/active MPTY without another call (see subclauses 1.2.1 and 1.3.1)."

Subclauses 1.2.1 and 1.3.1 include several different procedures for adding calls to the multiparty and removing calls. It is not clear from clause 1.4.1.2 whether it is allowed to disconnect a single party from the multiparty call (Clauses 1.2.1.3 and 1.3.1.4) when a single call also exists or whether it is only allowed to terminate the whole multiparty call (clauses 1.2.1.4 and 1.3.1.5) when a single call also exists.

GERAN 4 would very much welcome a clarification of this issue, as it impacts the validity of some test cases in the conformance test specification 51.010-1. GERAN 4 would also recommend a change to GSM 04.84 to reflect the outcome of this clarification.

3GPP TSG-GERAN WG4 **N4-010097**
Sophia Antipolis, France **(G4-000318)**
20-24 November 2000

Liaison Statement

From: 3GPP TSG GERAN-WG4

To: **3GPP TSG S-WG1**

Cc: **3GPP TSG N-WG4**

Subject: **Request for clarification on MPTY auxiliary state when only one remote party remains**

TSG GERAN WG4 seeks advice from TSG S-WG1 on the following issue.

GSM 02.84 from Phase 2 onwards, clause 1.3.8.2 Managing an active multiParty call: "During an active multiParty call, the served mobile subscriber shall be able to: (v) Disconnect a remote party: Explicitly release the remote parties on a one at a time basis. In the case when no remote parties remain, the MultiParty call is terminated."

From this statement, it is not clear, when only one remote party remains after explicitly releasing all other remote parties, whether this call should remain in auxiliary state "Call in MPTY" or not.

For example, if calls A-B and A-C are joined in a MPTY call, both calls will have auxiliary state "Call in MPTY". If call A-C is subsequently disconnected form the MPTY, does call A-B remain in auxiliary state "Call in MPTY"?

GERAN 4 cannot find further clarification in GSM 04.84 or other documents.

GERAN 4 would very much welcome clarification of this issue, as this issue affects several test cases in the conformance test specification 51.010-1.

GERAN4 recommends a modification to the Core Specifications to reflect this clarification .

3GPP TSG-CN4 **Tdoc N4-010160**
CN4#06 Meeting, Beijing, CHINA
15th January – 19th January 2001

Title: **LS for clarification of MPTY issues.**

Source: **TSG CN WG4**

To: **TSG SA WG1, TSG GERAN WG4**

Cc:

Contact Person:

Name: Nick Russell
E-mail Address: nick.russell@vf.vodafone.uk
Tel. Number: +44 (0)1635 682 699

---

1. Overall Description:

TSG CN WG4 thank GERAN 4 for their two liaison statements on the subject of MultiParty (MPTY). Please find a description of our findings below.

LS G4-000318, entitled "Request for clarification on MPTY auxiliary state when only one remote party remains"
When only one remote party remains after explicitly releasing all other remote parties, this call **shall** remain in auxiliary state "Call in MPTY". Only when there are no remote parties left in the MPTY shall the MPTY call be terminated. This can be verified in the SDL diagrams (Figure 1.2) in section 1.1 "Functions and information flows" of the stage 2 description of MPTY – GSM 03.84 or 3GPP TS 23.084.

LS G4-000317, entitled "Request for clarification on disconnecting Multiparty calls when a single call is active"
TSG CN WG4 believe that an inconsistency between the stage 1 and 3 documents and the stage 2 document has been identified.

In the stage 1 and 3 documents (GSM 02.84/3GPP TS 22.084 and GSM 04.84/3GPP TS 24.084) there is no description of whether or not the user is able to disconnect a single remote party in an active MPTY while a single held call exists or to disconnect a single remote party in a held MPTY while a single active call exists.

By contrast, in the stage 2 document (GSM 03.84/3GPP TS 23.084), section 1.1 "Functions and information flows", figure 1.2, sheets 4 and 8 (states "Held_MPTY_and_active_call" and "Active_MPTY_and_held_call" respectively) the overall SDL diagrams show that a single call within a MPTY call **can** be disconnected while a single active/held call exists.

Finally, it has also been identified that in the MMI specification (GSM 02.30/3GPP TS 22.030) the MMI is defined for the subscriber to disconnect a single remote party from an **active** MPTY call (regardless of whether or not there is a held single call) but there is no MMI defined for the subscriber to disconnect a specific party from a **held** MPTY call (regardless of whether or not there is an active single call).

2. Actions:

To TSG SA WG1:

Action for LS G4-000318: TSG CN WG4 consider that no action need be taken.

Action for LS G4-000317: TSG CN WG4 request clarification on whether or not the user is able to terminate a single remote party in an *active* MPTY while a single *held* call exists and whether or not the user is able to terminate a single remote party in a *held* MPTY while a single *active* call exists.

TSG CN WG4 also ask for any modifications to be made to the stage 1 of MPTY and the MMI specification (where appropriate) as far as back SA WG1 decide is necessary.

To TSG GERAN WG4:

Action for LS G4-000318: TSG CN WG4 consider that no further action need be taken on this issue.

Action for LS G4-000317: TSG CN WG4 ask GERAN WG4 to await a further response on this issue after they have received and processed a reply from SA WG1.

3. Attachments:

N4-010097 (G4-000318)
N4-010096 (G4-000317)

4. The next CN4 meeting

CN4 #07, 26th February – 2nd March 2001, Sophia Antipolis, France.

3GPP TSG-CN4 **Tdoc N4-010180**
CN4#06 Meeting, Beijing, CHINA
15th January – 19th January 2001

Title: **LS on proposed fix for GPRS Roaming issues.**

Source: **3GPP TSG CN WG4**

To: **3GPP TSG SA WG2**

Cc:

Contact Person:

Name: Nick Russell
E-mail Address: nick.russell@vf.vodafone.uk
Tel. Number: +44 (0)1635 682 699

---

1. Overall Description:

TSG CN WG4 recommend a solution to the problem (identified at TSG CN plenary #10) with GPRS mobile stations attempting to register in an SGSN of a VPLMN where there is no roaming agreement between the VPLMN and HPLMN operators for GPRS service. The problem occurs when the subscriber, normally allowed to roam in the CS domain of the VPLMN but not the PS domain of the same VPLMN, will be denied service from **both the PS and CS** domains of the VPLMN.

This is because the rejection cause “PLMN not allowed” is sent to the mobile, which causes it to delete GSM related parameters and to add the VPLMN into its ‘PLMN forbidden list’.

TSG CN WG4 have approved CRs to GSM 09.02 (R97 and R98) and TS 29.002 (R99 and Rel4) to define the behaviour of the MAP protocol layer in the SGSN so that if the SGSN cannot determine the HLR address to open the dialogue for GPRS location updating then it will indicate this explicitly to the requesting application (which is defined in GSM 03.60/23.060) rather than send it a “PLMN not allowed” message. The attached CRs define the behaviour of the SGSN application as "return an appropriate reject cause to the MS" (as is currently defined for the case where roaming is restricted in the SGSN because of an unsupported feature). Corresponding CRs to GSM 09.10 (R97 and R98) and TS 29.010 (R99) to show the mapping to the specific reject cause on the access interface are expected to be approved by CN4 and CN1 in time for submission to TSG-CN plenary #11.

2. Actions:

To TSG SA WG2:

Action: TSG CN WG4 ask TSG SA WG2 to approve the attached CRs (endorsed by TSG CN4) and present them to TSG-SA #11 for final approval.

3. Attachments:

N4-010091 (CR to GSM 03.60 R97)
N4-010092 (CR to GSM 03.60 R98)
N4-010093 (CR to 3GPP TS 23.060 R99)

4. The next CN4 meeting

CN4 #07, 26th February – 2nd March 2001, Sophia Antipolis, France.

3GPP TSG-CN4 **Tdoc N4-010203**
CN#06 Meeting , Beijing, CHINA
15th January – 19th January 2001

Source: **TSG CN WG 4**

Title: **Proposed Response to SA3 on SA3 agreements on MAPSec**

To: **TSG SA WG3**

Contact Person:
Name: Peter Schmitt
E-mail Address: peter.schmitt@icn.siemens.de
Tel. Number: +49 6621 169 152

TSG CN WG4 thank TSG SA WG3 for their LS on SA3 agreements on MAPSec [S3-000760] and provide the following answers, comments, questions and information:

- **Structure of Security Header**
  The attached CR 168r1 to 29.002 modifies the internal structure of the Security Header according to the SA3 agreements.
  Can SA3 please confirm that a single Initialisation Vector (IV) in the Security Header is sufficient, i.e. if in protection mode 2 both the encryption Algorithm and the Integrity/Authenticity Algorithm require an IV, the same IV will be used.

- **Algorithm Selection for MAP Security**
  The selected Encryption Algorithm (AES) and the selected Integrity/Authenticity Algorithm (AES-MAC) may be used with various key lengths, block lengths and modes of operations. Furthermore the length of the Integrity Check Value produced by AES-MAC is not fixed. The length of the additional message overhead introduced by MAPSec very much depends on the chosen block length (IV length, padding), mode of operation (IV present/absent, padding present/absent) and on the length of the Integrity Check Value. Concerns have been raised that the additional overhead may result in an available message length for the MAP application which does not allow a single Authentication Quintet to be carried in worst case scenarios.
  SA3 are asked to refine their algorithm selection by determining
  - the block length which is to be mandatorily supported,
  - the key length which is to be mandatorily supported,
  - the mode of operation for AES which is to be mandatorily supported,
  - the mode of operation for AES-MAC which is to be mandatorily supported,
  - the length of the Integrity Check Value which is to be mandatorily supported

  in a way which minimises the overhead as far as possible while ensuring an acceptable level of security.

Specification of MAP-Protection Profiles
In addition to the alternatives given in the LS from SA3, protection Modes may also be specified against components of operations. This can be used to allow different components of the same operation, which are carried in different messages sent in different directions and thus being protected by different SAs, to be protected independently from each other.

If this alternative is chosen, CN4 proposes to standardise a limited number of profiles for Release 4. An example is given in the table:

Profile number	InfoRetrievalContext-v3			InterVlrInfoRetrievalContext-v3			AnyTimeInfoHandlingContext-v3		
	SAI invoke	SAI result	SAI error	SI invoke	SI result	SI error	ATM invoke	ATM result	ATM error
1	PM 1	PM 2	PM 0	PM 1	PM 2	PM 0	PM 1	PM 1	PM 0
2	PM 1	PM 1	PM 0	PM 1	PM 1	PM 0	PM 1	PM 1	PM 0
3	PM 2	PM 2	PM 0	PM 2	PM 2	PM 0	PM 2	PM 2	PM 0

SAI: SendAuthenticationInfo
SI: SendIdentification
ATM: AnyTimeModification
PM: Protection Mode

- **Use of Protection Mode 0**
  Protection mode 0 is relevant for cases where some but not all components need protection within a dialogue (e.g. error components). In cases where no component of a dialogue needs protection it is of course better and avoiding overhead not to make use of the MAP Security mechanism at all, rather than using the MAP security mechanism and "protecting" all components with protection mode 0.

3GPP TSG-CN WG4 **Tdoc 3GPP N4-010204**
Beijing, China
15 – 19 January 2001

Source: TSG-CN WG4[1]

Title: LS on Maximum size of LCS clients

To: TSG-SA 1, TSG-SA 2

TSG CN WG4 has discussed the matter of maximum numbers of LCS clients and likes to inform SA1 and SA2 about the outcome of these discussions.

CN4 likes to inform SA1 and SA2 that there is protocol limitations (mainly segmentation of the messages) that have to be concidered when the maximum number of LCS clients is defined. CN4 has been notified of the proposal made by DoCoMo on SA1 mailing list (maximum number shall be 40) and CN4 agreed to use this maximum number as working assumption pending on the SA 1 approval of this service requirement.

40 clients can be transferred with MAP protocol only if the White Book SCCP is used. CN4 likes to remind that 3GPP TS 29.002 mandates the use of White Book SCCP from 1st of July 2002. If the Blue Book SCCP is used, only 5 clients can be transferred without specifying protocol level segmentation which is not recommended by CN4.

CN4 recommendation is that the maximum LCS clients is 40 and the segmentation problems are solved by using White Book SCCP.

The next CN4 meetings are (Release 4 adhoc) on 13- 15 February 2001 and (CN4 #07), 26th February – 2nd March 2001.

1 Contact: Teemu Mäkinen, email: teemu.makinen@nokia.com

3GPP TSG-CN4 Ad Hoc meeting
Madrid, Spain
13th – 15th February 2001

Tdoc N4-010282

Title: **LS response on GTP-U version negotiation**

Source: **TSG_CN4**

To: **TSG_RAN3**

Cc:

Contact Person:
Name: **Toshiyuki Tamura**
E-mail Address: **tamurato@nsf.ncos.nec.co.jp**
Tel. Number: +81 471-85-6901

TSG CN4 thanks TSG RAN3 for their LS TSGR3#18(01) 0310 on GTP-U version negotiation.

TSG CN4 believes that the extension header mechanism which has been defined in GTP version 1 can be used for future enhancements to GTP-U. In that sense, the GTP-U version will stay the same for the foreseeable future. Therefore, the risk of not having the version negotiation mechanism in GTP-U is acceptably low.

Thus, TSG CN4 concluded that **the GTP-U version negotiation mechanism does not need to be introduced.**

The following answers are provided based on the conclusion described above.

1) RAN-WG3 has become aware of the fact that GTP-U no longer has version supported message. Is this decision taken with knowledge about the Iu interface, and especially the forwarding tunnel, where GTP-C is not present?

ANSWER: Yes, TSG CN4 had recognised that the current RANAP does not have an ability to negotiate the GTP-U version. However, for the reason described above, TSG CN4 believe that not having the GTP-U version negotiation mechanism in RANAP will not cause problems.

2) If the answer of 1) is no, does N4 see a need to have GTP-U version negotiation for the forwarding tunnel?

ANSWER: See answer for Q1).

3) If the GTP-U version negation is needed, CN-WG4 could be kindly asked if CN WG4 has a view on how the GTP-U version negotiation could work in the Inter-SGSN Relocation?

ANSWER: See answer for Q1).

4) RAN-WG3 has discussed shortly a method for GTP-U version negotiation on RANAP, i.e. indicate the GTP-U version in relevant RANAP messages (see attached R3-010074 for detail). However, this solution is against the main design principle applied in RAN WG3 specification work, i.e. the independence of Radio Network Layer and Transport Network Layer. Following this principle, the GTP-U version negotiation should be on GTP (i.e. the Transport Network Layer) level. Would CN-WG4 give opinion on this solution?

ANSWER: See answer for Q1).

5) When in the absence of GTP-C, how does the node act when an unsupported version

ANSWER: Because of the conclusion described above, TSG CN4 believes that the node will not receive a message formatted with unsupported version. Therefore, immediate action to treat this situation is not necessary.

3GPP TSG-CN4 **Tdoc N4-010283**
CN4 Ad Hoc Meeting , Madrid, SPAIN
13th Ferbuary – 15th February 2001

Source:	**TSG-CN WG4**
To:	**TSG-SA WG4, TSG-RAN WG2, TSG-T, TSG-GERAN, TSG-RAN WG1**
CC:	**TSG-CN WG1**
Title:	**LS for "**Reply on Default Configurations for Handover"
Contact:	Tellabs (Prem.Tirilok@tellabs.com) and Ericsson (Philip.Hodges@ericsson.com.au)

TSG-CN WG4 (CN4) would like to thank TSG-SA WG4 (SA4) for their LS (N4-010218 / S4-01022) on default configurations for handover from GSM to UMTS.

CN4 understands the requirement for this addition of this new UMTS_AMR2 codec type and is in support of the proposal in principle. However, CN4 would like to understand if this requires the addition of a new Codec Type ID, i.e. in the codec list 26.103 and support in TFO enabled Transcoders in the core network equipment, when generating TFO_REQ, TFO_REQ_L and similar messages mentioned in TS 28.062.

3GPP TSG-CN4 **Tdoc N4-010284**
CN4 Rel-4 Ad Hoc Meeting, Madrid, SPAIN
13th February – 15th February 2001

Title: **LS highlighting requirements to RAN WG3 for SRNS Relocation withTrFO**

Source: **TSG_CN WG4**

To: **TSG_RAN WG3**

Cc: **TSG_SA WG2, TSG_CN WG1**

Contact Person:

Name: **Mr Phil Hodges**
E-mail Address: **philip.hodges@ericsson.com.au**
Tel. Number: +61 3 9911 3414

---

1. Overall Description:

CN4 has approved CRs describing the handling of TrFO calls during SRNS relocation in stage 2 specification 23.153. For Inter-MSC serving area relocations the specification uses direct RANAP signalling as for Intra-MSC serving area relocations. This is in accordance with the agreement made by SA2 as described in their LS (S2-002000, N4-001099), a copy of which was also sent to RAN3.

CN4 has thus assumed that the support of this functionality can be achieved in RAN3 for Rel4, the scope of the requirement being the support of a 1 to many relationship for RNC to MSC SCCP connections.

2. Actions:

To TSG RAN3:

ACTION: TSG_N WG4 asks **TSG RAN WG3** to confirm that they accept and are addressing the requirements needed by CN4 for this functionality.

3. Attachments:

N4-001099

4. The next CN4 meeting

CN4 WG meeting #7, Sophia Antipolis, 26th Feb-02nd Mar 2001

3GPP TSG-CN4 Ad Hoc meeting
Madrid, Spain
13th – 15th February 2001

Tdoc N4-010285

Title: **LS response on Enhancement of LCS functionality in Rel-4**

Source: **TSG_CN4**

To: **TSG_SA2**

Cc: **TSG_SA1**

Contact Person:
Name: **Toshiyuki Tamura**
E-mail Address: **tamurato@nsf.ncos.nec.co.jp**
Tel. Number: +81 471-85-6901

TSG CN4 thanks TSG SA2 for their LS S2-010060 on Enhancement of LCS functionality in Rel-4.

TSG CN4 accepted the SA2 suggestion to continue our work based on the description in the Annex of 23.271. TSG CN4 also recognised that the necessary stage 3 CRs could be approved in TSG CN4 on the basis that the current informative ANNEX in 23.271 would be approved to be moved to the normative description.

According to the current schedule in TSG CN4, the final review for corresponding stage 3 CRs will be made in our next TSG CN4 meeting between 26th of February and 2nd of March in Sophia Antipolis, France.

Due to the fact that two meetings TSG CN4 and TSG SA2 will take place in the same week, TSG CN4 kindly requests TSG SA2 to inform TSG CN4 of the status of the ANNEX in 23.271 as soon as concluded in TSG SA2.

3GPP TSG-CN4 **Tdoc N4-010291**
CN4 Rel-4 Ad Hoc Meeting, Madrid, SPAIN
13th February – 15th February 2001

Title: ***DRAFT*** **LS reply to SA3 on request for information to complete security work items**

Source: **TSG_CN WG4**

To: **TSG_SA WG3**

Cc: **-**

Contact Person:

Name: **Mr Phil Hodges**
E-mail Address: **philip.hodges@ericsson.com.au**
Tel. Number: +61 3 9911 3414

---

1. Overall Description:

CN4 thanks SA3 for their LS (S3-000742/N4-010229) regarding security. SA3 asked CN4 for input regarding the prevention of user fraud concerning TrFO OoBTC solution.

CN4 does not foresee any specific fraud issues with respect to TrFO connections.

2. Actions:

To TSG RAN3:

ACTION: TSG_N WG4 asks **TSG SA WG3** to describe any specific areas of concern they have with respect to TrFO if any have been raised by their group.

3. Attachments:

None.

4. The next CN4 meeting

CN4 WG meeting #7, Sophia Antipolis, 26th Feb-02nd Mar 2001

3GPP TSG-CN4 **Tdoc N4-010302**
CN4 Rel-4 Ad Hoc Meeting, Madrid, SPAIN
13th February – 15th February 2001

Title: Response to SA1 LS (Tdoc S1-010219) on maximum number of LCS clients in the "privacy client list".

Source: **TSG_CN WG4**

To: **TSG_SA WG1, TSG SA WG2**

Cc:

Contact Person:

Name: **Mr John Menard**
E-mail Address: **jmenard@lucent.com**
Tel. Number: +1 630-979-6376

CN4 would like to thank SA1 for their LS on the subject of the maximum number of LCS clients in the "privacy client list". CN4 wishes to acknowledge:

- SA1's desire that there be no upper bound to the maximum number of LCS clients in the "privacy client list".
- SA1's requirement that the lowest value of such upper bound is 20.

CN4 is in complete agreement with the objective of SA1 in not having a technology limitation being translated into a service requirement. However, 3GPP has already imposed such a technology limit on itself when it selected Blue Book SCCP and now White Book SCCP for the transportation of MAP and CAP messages. As previously noted, preliminary analysis has shown that the use of Blue Book results in a limit of 5 LCS "privacy clients" whereas the use of White Book results in a limit of approximately 40 "privacy clients".

While White Book SCCP is being used, this message length limit cannot be avoided.

Therefore, all 3GPP SCCP applications have the problem of what to do when they need to transmit a message whose size exceeds the maximum allowed by 3GPP's chosen technology. In the case of the "privacy client list", CN4 believes that this 3GPP SCCP application will need to produce a shorter and probably incomplete list from the desired list. CN4 believes that the process of generating this shorter list from the complete list should be standardized to ensure consistency and predictability in the behaviour of this 3GPP SCCP application no matter where this application may be executed. CN4 believes that since SA1 has the best understanding of the implications of shortening the "privacy list", it should undertake the task of defining this algorithm.

ACTION: TSG CN WG4 asks **TSG SA WG1** to confirm their acknowledgement of TSG_CN WG4's statement regarding 3GPP's self-imposed technology limit, and

ACTION: TSG CN WG4 asks **TSG SA WG1** to produce the "privacy client list reduction" algorithm so that **TSG SA WG2** can include this algorithm in TS 23.271.

Next CN4 meeting

CN4 WG meeting #7, Sophia Antipolis, 26th Feb-02nd Mar 2001

3GPP TSG-CN4 **Tdoc N4-010307**
CN4 Rel-4 Ad Hoc Meeting, Madrid, SPAIN
13th February – 15th February 2001

Title: ***DRAFT*** **LS Response Lawful Intercept support on the Mc interface**

Source: **TSG CN WG4**

To: **TSG SA WG3**

Cc:

Contact Person:

Name: **Ms Elena Garcia-Mendive**
E-mail Address: **Elena.Garcia-Mendive@eed.ericsson.se**
Tel. Number: +49 2407 575 205

---

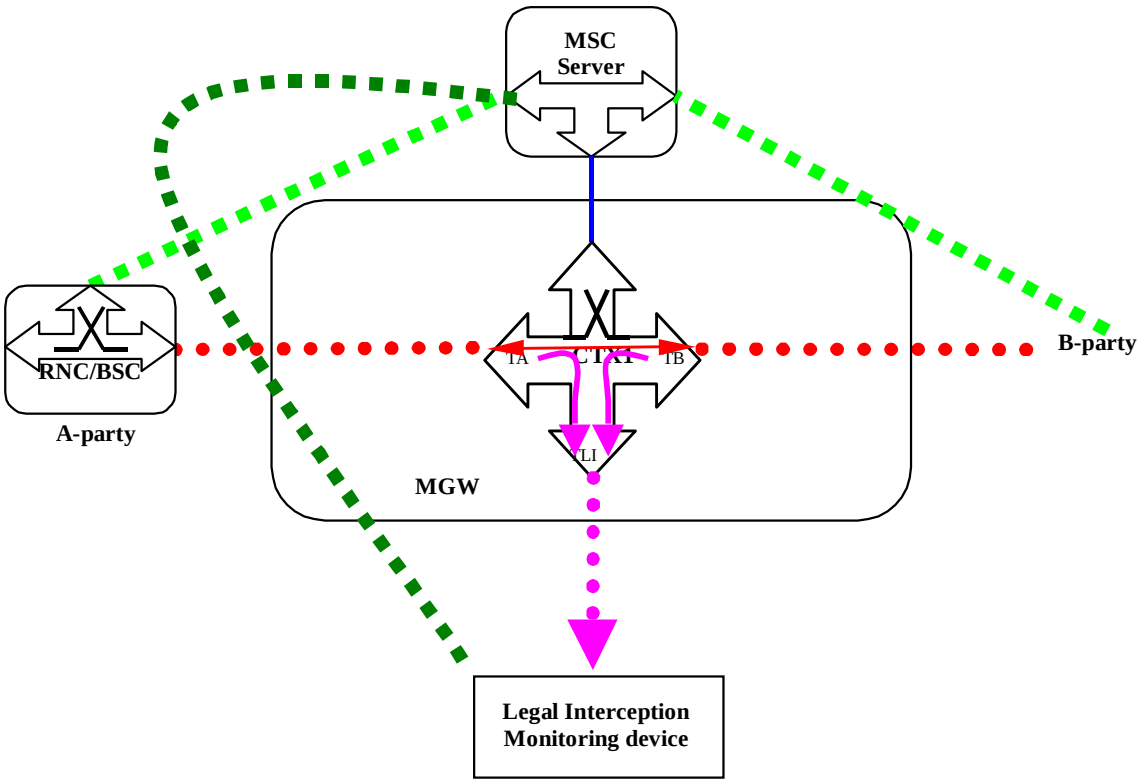
1. Overall Description:

TSG CN WG4 thanks TSG SA3 for their liaison statement on the subject of 'Lawful Intercept support on the Mc interface'. Please find a description of our findings below.

We identified the following nodes involved in a call subject to legal interception: the MSC server, the MGW and the LI monitoring device as shown in the figure. **We assume there is an X3 interface towards the MGW with the same characteristics as the other bearer interfaces on the MGW**. In such scenario, your requirement is 'S3 LI solicits your support in developing such as standard intercept control message to invoke intercept in the MGW'.

There is a mechanism already provided on the Mc interface (ITU-T H.248 protocol) to add a new termination within a context, TLI in the figure below. This allows the legal interception of one party or both (even all the parties involved in MPTY) via the so-called 'topology' concept. This new termination shall be connected to the Legal Interception monitoring device.

In the figure below the green 'squared' lines represent the signalling and the red and pink 'dotted' lines represent the bearer. The blue line between the MSC server and the MGW represents the Mc interface. The arrows within the context CTX1 represent the internal topology between every two terminations: ‘bothway through-connected’ between TA and TB; 'forward through-connected' from TA to TLI; and 'forward through-connected' from TB to TLI.



We have assumed that the encoding at the termination TLI is ITU-T G.711, and therefore we do not see the need for a new 'standard intercept control message' since the mechanisms which are already in the standard protocol over the Mc interface (ITU-T H.248) meet these requirements.

2. Actions:

To TSG SA3:

ACTION: TSG CN WG4 asks TSG SA WG3 to confirm our working assumption. If TSG SA WG3 is not able to confirm this assumption, we believe we'll need a join meeting to resolve this issue. This will require Legal Interception for BI CS CN will be postponed to REL-5.

3. Attachments:

None.

4. The next CN4 meeting

CN4 #07, 26th February – 2nd March 2001, Sophia Antipolis, France.

CN4 #8, 14th –18th May 2001, USA.

3GPP TSG-CN WG4 **Tdoc N4-010439**
CN4 Meeting #7, Sophia Antipolis, FRANCE
26th February – 2nd March 2001

Title: **LS on handling of an error case for authentication set retrieval**

Source: **TSG-CN WG4**

To: **TSG-SA WG2**

Contact Person:
Name: **Ian Park**
E-mail Address: **ian.park@vf.vodafone.co.uk**
Tel. Number: +44 1635 673 527

---

1. Overall Description:

TSG-CN WG4 have considered a set of change requests which are intended to deal with an error case for GPRS roaming. The root cause of the problem is a situation where two operators have a roaming agreement for CS services but not for GPRS services. More details are given in the attached LS from CN WG1.

During their work on this problem, TSG-CN WG4 identified a particular error case which can arise where no GPRS roaming agreement exists between the VPLMN and HPLMN operators: the SGSN does not have the necessary data transcript to derive an E.214 HLR address for the SCCP signalling from the SGSN to the HLR, so it cannot signal to the HLR to request authentication sets. The description of the handling for this error case requires CRs to GSM 03.60 for Release 97 and Release 98, and to TS 23.060 for Release 99. TSG-CN WG4 have reviewed the draft CRs, and endorsed them; however, since TSG-SA WG2 have responsibility for GSM 03.60 and TS 23.060, the CRs need to be agreed by TSG-SA WG2 before they are presented for approval to the TSG. The companion CRs to GSM 09.02 for Release 97 and Release 98, and to TS 29.002 for Release 99 and Release 4, have been reviewed and agreed by TSG-CN WG4. They will be presented for approval at TSG-CN #11.

2. Actions:

TSG-CN WG4 ask **TSG SA WG2** to consider the attached CRs to GSM 03.60 and TS 23.060, and forward them to TSG-SA #11 for final approval.

3. Attachments:

Tdoc N4-010440: CR to GSM 03.60 (R97) on Failure of Authentication Parameter GPRS when HLR is not reachable;
Tdoc N4-010441: CR to GSM 03.60 (R98) on Failure of Authentication Parameter GPRS when HLR is not reachable;
Tdoc N4-010442: CR to TS 23.060 (R99) on Failure of Authentication Parameter GPRS when HLR is not reachable.

4. The next TSG-CN WG4 meeting

The next TSG-CN WG4 meeting is scheduled for 14 – 18 May 2001 in Puerto Rico.

3GPP TSG-CN-WG1, Meeting #15
15-19 January 2001, Beijing, China

Tdoc N1-010211

From: TSG CN WG1

To: TSG CN WG4, TSG SA WG1, TSG GERAN WG2

CC: TSG SA, TSG CN

Title: LS on Problem with GPRS and Roaming

Date: 18-January-2001

Contact: Sophie Aveline, France Telecom [sophie.aveline@francetelecom.fr]

Attachments: N1-010216, (04.08 CR)
N1-010215, N1-010223 (03.22 CRs)

During TSG CN Plenary #10 and during TSG SA Plenary #10, Tdoc NP-00697 and Tdoc SP-00666 respectively raise the same very important problem concerning GPRS and roaming situation. This problem, which has been experienced from the deployment of GPRS in live networks, has been further analysed by TSG CN WG1 and can be summarised as follows:

Operator A has a Roaming agreement with operator B, but only for Circuit Switched services not for GPRS (both networks supporting GPRS).
The customer moves from operator A's coverage to operator B's coverage. Operator B should accept that customer's attach/registration attempts on network B for circuit switched services, but should reject the GPRS attach.

Instead of such behaviour, two different implementations have been identified:
- *According to 3GPP specifications, the customer is denied from the whole operator B's network (CS and PS domains) (error cause #11 "PLMN not allowed" of TS 04.08 R'97)*
- *A manufacturer's specific implementation tries to avoid such problem sending another error cause value (#7 "GPRS service not allowed" of TS 04.08 R'97), but according to the TS 04.08 the MS is not allowed to try anymore to attach to a PS domain of any GSM network unless it is switched off and on.*

Consequently, if there is only a roaming agreement for CS services but not for PS service (GPRS) with the visited network, there does not exist any suitable cause value with which PS attach can be rejected without impact on both the GSM services and the GPRS services in other networks.

In order to solve the problem a **new rejection cause** value "**GPRS services not allowed in this PLMN**"(**#14**) has been introduced. This new rejection cause can be sent to the MS during GPRS attach, detach and RAU if a visited PLMN does not offer GPRS roaming to that MS. A list of "forbidden PLMNs for GPRS service" has been introduced in 03.22(23.122) which must at least consist of one entry.

Relevant CRs have been agreed by CN1 to 04.08 and 03.22 for all releases from R97 onwards. Attached to this liaison is Tdoc N1-010216 containing the CR on 04.08 Release 97 (the companion CRs are in Tdoc N1-010219, Tdoc N1-010220 and Tdoc N1-010221).The CR on TS 03.22 R97 is attached to this liaison in Tdoc N1-010215 (the companion CRs are in Tdoc N1-010223 and Tdoc N1-010224).

1. TSG CN WG1 would like to ask TSG CN WG4 to proceed with the necessary work under their responsibility to support this solution to solve this GPRS roaming problem.

2. TSG CN WG1 would like to ask TSG SA WG1 to proceed to the relevant modifications, if needed, to TS 02.11 R'97, TS 02.11 R'98, TS 22.011 R'99 and 22.011 R4 as the corresponding stage 3 needed some modifications for the implementation of the solution of this GPRS roaming problem. The relevant CR on TS 03.22 Release 97 is attached to this liaison in Tdoc N1-010215 (the companion CRs are in Tdoc N1-010223 and Tdoc N1-010224).

3. TSG CN WG1 would like to ask TSG GERAN WG2 to endorse the CRs on 03.22 as TSG GERAN WG2 has the prime responsibility for 03.22.

3GPP TSG-CN4 Meeting #07 **Tdoc N4-010440**
Sophia Antipolis, France, 26th February 2nd March 2001

CR-Form-v3

CHANGE REQUEST

⌘ **03.60** **CR** **???** ⌘ rev ⌘ Current version: **6.7.0** ⌘

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

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

Title:	⌘	Failure of Authentication Parameter GPRS when HLR is not reachable
Source:	⌘	France Telecom
Work item code:	⌘	GPRS R97
Date:	⌘	26 Feb 2001
Category:	⌘	**F** Essential Correction
Release:	⌘	R97

Use one of the following categories:
F *(essential 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:	⌘	No Error case was described for the Obtain Authentication Parameter in the SGSN if the SGSN cannot address the subscribers HLR.
Summary of change:	⌘	Show the use of the error "Unknown HLR" for Authentication Procedures
Consequences if not approved:	⌘	Risk of different implementations due to a lack of description

Clauses affected:	⌘	6.8.1; 6.9.1.2.2; 6.9.1.3.1; 6.9.1.3.2		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	GSM 09.02 GSM 09.10
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.8.1 Authentication of Subscriber

Authentication procedures already defined in GSM shall be used, with the distinction that the procedures are executed from the SGSN. The GPRS Authentication procedure performs subscriber authentication, or selection of the ciphering algorithm and the synchronisation of the start of ciphering, or both. Authentication triplets are stored in the SGSN. The MSC/VLR shall not authenticate the MS via the SGSN upon IMSI attach, nor location update, but may authenticate the MS during CS connection establishment. Security-related network functions are described in GSM 03.20 [6].

The Authentication procedure is illustrated in Figure 1. Each step is explained in the following list.

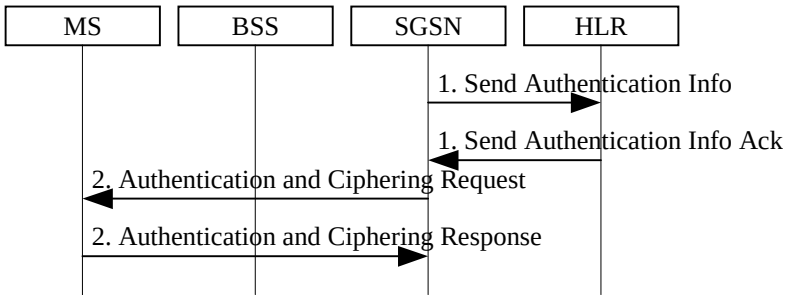


Figure 1: Authentication Procedure

1) If the SGSN does not have previously stored authentication triplets, a Send Authentication Info (IMSI) message is sent to the HLR. The HLR responds with a Send Authentication Info Ack (Authentication Triplets) message. Each Authentication Triplet includes RAND, SRES, and Kc.

2) The SGSN sends an Authentication and Ciphering Request (RAND, CKSN, Ciphering Algorithm) message to the MS. The MS responds with an Authentication and Ciphering Response (SRES) message.

The MS starts ciphering after sending the Authentication and Ciphering Response message. The SGSN starts ciphering when a valid Authentication and Ciphering Response is received from the MS. In the routeing area update case, if ciphering was used before the routeing area update, and if the Authentication procedure is omitted, then the SGSN shall resume ciphering with the same algorithm when a ciphered Routeing Area Update Accept message is sent, and the MS shall resume ciphering when a ciphered Routeing Area Update Accept message is received.

If the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue, the Authentication Procedure fails.

**** Next modified section ****

6.9.1.2.2 Inter SGSN Routeing Area Update

...

3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.
If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
A reject shall be returned to the MS with an appropriate cause.

...

**** Next modified section ****

6.9.1.3.1 Combined Intra SGSN RA / LA Update

...

2) Security functions may be executed. This procedure is defined in subclause "Security Function".
If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
A reject shall be returned to the MS with an appropriate cause.

...

**** Next modified section ****

6.9.1.3.2 Combined Inter SGSN RA / LA Update

...

3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.
If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
A reject shall be returned to the MS with an appropriate cause.

...

3GPP TSG-CN4 Meeting #07 **Tdoc N4-010441**
Sophia Antipolis, France, 26th February 2nd March 2001

CR-Form-v3

CHANGE REQUEST

⌘ **03.60** **CR** **???** ⌘ rev ⌘ Current version: **7.5.0** ⌘

*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:	⌘	Failure of Authentication Parameter GPRS when HLR is not reachable
Source:	⌘	France Telecom
Work item code:	⌘	GPRS R97
Date:	⌘	26 Feb 2001
Category:	⌘	**A**
Release:	⌘	R98

Use one of the following categories:
F *(essential 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:	⌘	No Error case was described for the Obtain Authentication Parameter in the SGSN if the SGSN cannot address the subscribers HLR.
Summary of change:	⌘	Show the use of the error "Unknown HLR" for Authentication Procedures
Consequences if not approved:	⌘	Risk of different implementations due to a lack of description

Clauses affected:	⌘	6.8.1; 6.9.1.2.2; 6.9.1.3.1; 6.9.1.3.2		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	GSM 09.02 GSM 09.10
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.8.1 Authentication of Subscriber

Authentication procedures already defined in GSM shall be used, with the distinction that the procedures are executed from the SGSN. The GPRS Authentication procedure performs subscriber authentication, or selection of the ciphering algorithm and the synchronisation of the start of ciphering, or both. Authentication triplets are stored in the SGSN. The MSC/VLR shall not authenticate the MS via the SGSN upon IMSI attach, nor location update, but may authenticate the MS during CS connection establishment. Security-related network functions are described in GSM 03.20 [6].

The Authentication procedure is illustrated in Figure 1. Each step is explained in the following list.

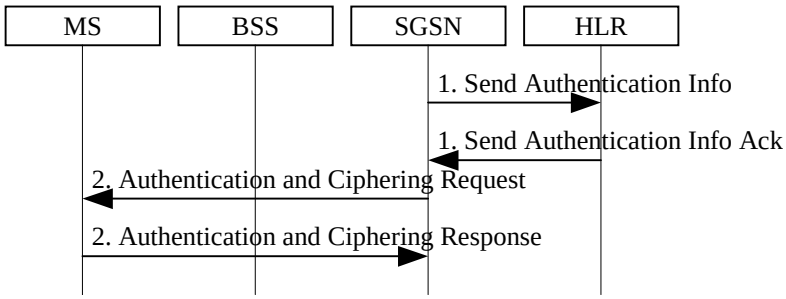


Figure 1: Authentication Procedure

1) If the SGSN does not have previously stored authentication triplets, a Send Authentication Info (IMSI) message is sent to the HLR. The HLR responds with a Send Authentication Info Ack (Authentication Triplets) message. Each Authentication Triplet includes RAND, SRES, and Kc.

2) The SGSN sends an Authentication and Ciphering Request (RAND, CKSN, Ciphering Algorithm) message to the MS. The MS responds with an Authentication and Ciphering Response (SRES) message.

The MS starts ciphering after sending the Authentication and Ciphering Response message. The SGSN starts ciphering when a valid Authentication and Ciphering Response is received from the MS. In the routeing area update case, if ciphering was used before the routeing area update, and if the Authentication procedure is omitted, then the SGSN shall resume ciphering with the same algorithm when a ciphered Routeing Area Update Accept message is sent, and the MS shall resume ciphering when a ciphered Routeing Area Update Accept message is received.

If the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue, the Authentication Procedure fails.

**** Next modified section ****

6.9.1.2.2 Inter SGSN Routeing Area Update

...

3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.
If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
A reject shall be returned to the MS with an appropriate cause.

...

**** Next modified section ****

6.9.1.3.1 Combined Intra SGSN RA / LA Update

...

2) Security functions may be executed. This procedure is defined in subclause "Security Function".
If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
A reject shall be returned to the MS with an appropriate cause.

...

**** Next modified section ****

6.9.1.3.2 Combined Inter SGSN RA / LA Update

...

3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.
If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
A reject shall be returned to the MS with an appropriate cause.

...

3GPP TSG-CN4 Meeting #07 **Tdoc N4-010441**
Sophia Antipolis, France, 26th February 2nd March 2001

CR-Form-v3

CHANGE REQUEST

⌘ **23.060** **CR** **???** ⌘ rev ⌘ Current version: **3.6.0** ⌘

*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:	⌘	Failure of Authentication Parameter GPRS when HLR is not reachable
Source:	⌘	France Telecom
Work item code:	⌘	GPRS R97
Date:	⌘	26 Feb 2001
Category:	⌘	**A**
Release:	⌘	R99

Use one of the following categories:
F *(essential 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:	⌘	No Error case was described for the Obtain Authentication Parameter in the SGSN if the SGSN cannot address the subscribers HLR.
Summary of change:	⌘	Show the use of the error "Unknown HLR" for Authentication Procedures
Consequences if not approved:	⌘	Risk of different implementations due to a lack of description

Clauses affected:	⌘	6.8.1; 6.9.1.2.2; 6.9.1.3.1; 6.9.1.3.2		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	GSM 29.002 GSM 29.010
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.8.1 Authentication

The Authentication function includes two types of authentication: "UMTS authentication" and "GSM authentication".

"UMTS authentication" implies mutual authentication, i.e., authentication of the MS by the network and authentication of the network by the MS. It also implies establishment of a new UMTS ciphering key (CK) and integrity key (IK) agreement between the SGSN and the MS.

"GSM authentication" implies authentication of the MS by the network and establishment of a new GSM ciphering key (Kc) agreement between the SGSN and the MS.

6.8.1.1 Authentication of GSM Subscriber

Authentication procedures already defined in GSM shall be used, with the distinction that the procedures are executed from the SGSN. The GPRS Authentication procedure performs subscriber authentication, or selection of the ciphering algorithm and the synchronisation of the start of ciphering, or both. Authentication triplets are stored in the SGSN. The MSC/VLR shall not authenticate the MS via the SGSN upon IMSI attach, nor location update, but may authenticate the MS during CS connection establishment. Security-related network functions are described in GSM 03.20 [6].

The Authentication of GSM Subscriber procedure is illustrated in figure 27.

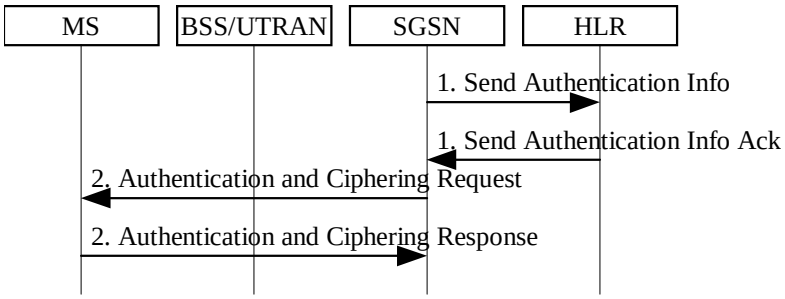


Figure 1: Authentication of GSM Subscriber Procedure

1) If the SGSN does not have previously stored authentication triplets, a Send Authentication Info (IMSI) message is sent to the HLR. The HLR responds with a Send Authentication Info Ack (Authentication Triplets) message. Each Authentication Triplet includes RAND, SRES, and Kc.

2) The SGSN sends an Authentication and Ciphering Request (RAND, CKSN, Ciphering Algorithm) message to the MS. The MS responds with an Authentication and Ciphering Response (SRES) message.

In GSM, the MS starts ciphering after sending the Authentication and Ciphering Response message as described in subclause "Start of Ciphering".

In UMTS, the 3G-SGSN and the MS shall generate the UMTS CK and IK from the GSM Kc using the standardised conversion functions specified for this purpose in 3G TS 33.102.

In UMTS, the start of ciphering is controlled by the security mode procedure described in 3G TS 33.102.

If the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue, the Authentication of GSM Subscriber Procedure fails.

6.8.1.2 Authentication of UMTS Subscriber

The UMTS authentication procedure is described in 3G TS 33.102. The UMTS authentication procedure executed from the SGSN performs both the mutual authentication and security keys agreement. Authentication quintuplets are stored in the SGSN. The MSC/VLR shall not authenticate the MS via the SGSN upon IMSI attach nor upon location update, but may authenticate the MS during CS connection establishment.

The Authentication of UMTS Subscriber procedure (USIM) is illustrated in figure 28.

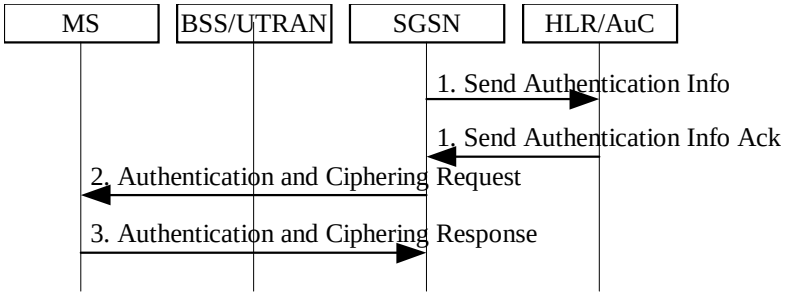


Figure 2: Authentication of UMTS Subscriber Procedure

1) If the SGSN does not have previously stored UMTS Authentication Vectors (quintuplets), a Send Authentication Info (IMSI) message is sent to the HLR. Upon receipt of this message for a UMTS user, the HLR/AuC responds with a Send Authentication Info Ack message including an ordered array of quintuplets to the SGSN. Each quintuplet contains RAND, XRES, AUTN, CK, and IK. The generation of quintuplets in HLR/AuC for a UMTS user is performed as specified in 3G TS 33.102.

2) At authentication of a UMTS subscriber, the SGSN selects the next in-order quintuplet and transmits the RAND and AUTN, that belong to this quintuplet, to the MS in the Authentication and Ciphering Request (RAND, AUTN, CKSN) message. The SGSN also selects a ciphering key sequence number, CKSN, and includes this in the message.

3) At reception of this message, the USIM in the MS verifies AUTN and, if accepted, the USIM computes the signature of RAND, RES, in accordance with 3G TS 33.102. If the USIM considers the authentication being successful the MS returns an Authentication and Ciphering Response (RES) message to the SGSN. The USIM in the MS computes then also a new Ciphering Key, CK, and a new Integrity Key, IK. These keys are stored together with the CKSN until CKSN is updated at the next authentication.

   If the USIM considers the authentication being unsuccessful, e.g., in case of an authentication synchronisation failure, the MS returns the Authentication and Ciphering Failure message to the SGSN. The actions then taken are described in 3G TS 33.102.

In GSM, the SGSN and the MS shall generate the Kc from the UMTS CK and IK using the standardised conversion function specified for this purpose in 3G TS 33.102.

If the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue, the Authentication of UMTS Subscriber Procedure fails.

**** Next modified section ****

6.9.1.2.2 Inter SGSN Routeing Area Update

...

3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.
   If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
   A reject shall be returned to the MS with an appropriate cause.

...

**** Next modified section ****

6.9.1.3.1 Combined Intra SGSN RA / LA Update

...

2) Security functions may be executed. This procedure is defined in subclause "Security Function".
If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
A reject shall be returned to the MS with an appropriate cause.

...

**** Next modified section ****

6.9.1.3.2 Combined Inter SGSN RA / LA Update

...

3) Security functions may be executed. These procedures are defined in subclause "Security Function". Ciphering mode shall be set if ciphering is supported.
If the security functions fail (e.g. because the SGSN cannot determine the HLR address to establish the Send Authentication Info dialogue), the Inter SGSN RAU Update procedure fails.
A reject shall be returned to the MS with an appropriate cause.

...