3GPP TSG CN Plenary Meeting #22 **NP-030495**
10th – 12th December 2003 Maui, USA.

Source: TSG CN WG4

Title: Liaison statements after CN#21

Agenda item: 6.4.1

Document for: APPROVAL

Tdoc	Tdoc Title	LS to	LS cc	LS Attachment
N4-031152	LS to SA3 on Clarification on use of Re-attempt Information element in Authentication Failure Report service	SA3		
N4-031289	LS on Special-RAND mechanism	SA3	CN1, GERAN2, T2	N4-031315
N4-031320	LS on Clarification for the WLAN D'/Gr' interface standardization	SA2		
N4-031351	LS on identifying MMS Enabled devices and MMS Capabilities of those devices	T2	SA1, SA2	N4-031328
N4-031352	LS to SA2 changes in MBMS activation procedures	SA2		
N4-031367	Response LS To GSMA on DNS top level domains	GSMA IREG PACKET	CN	
N4-031387	LS (S5-038444) on Rel-6 Subscriber and Equipment Trace impacts to the Core Network from WG SA5	SA5	CN1, CN2	

3GPP TSG CN WG4 Meeting #21 ***N4-031152***
Bangkok, Thailand, 27th – 31st October 2003

Title: **LS to SA3 on Clarification on use of Re-attempt Information element in Authentication Failure Report service**

Release: **6**

Work Item: **Security**

Source: **NEC (TSG CN4)**

To: **TSG SA3**

Cc:

Contact Person:
Name: Toshiyuki Tamura
Tel. Number: +81-4-7185-7167
E-mail Address: tamurato@aj.jp.nec.com

Attachments: **None**

1. Overall Description:

It was discussed in CN4#21 meeting in Bangkok that the use of the 'Re-attempt' parameter in Authentication Failure Report Service is not clear in current specifications how it could be used. Therefore, TSG CN4 kindly ask TSG SA3 to provide guidance on this question.

2. Background

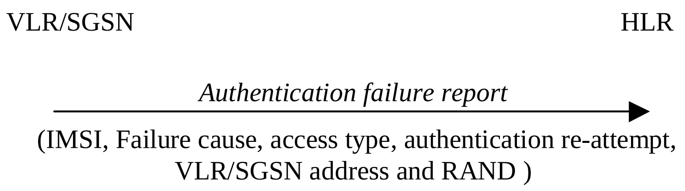
The 'Re-attempt' parameter was introduced as the REL4 feature about 2 years ago. This parameter is used in Authentication Failure Report Service in order to indicate whether the failure occurred in a normal authentication attempt or in an authentication reattempt (there was a previous unsuccessful authentication). However, it is not clear for NEC what is the “normal authentication attempt” meant and what is the “an authentication reattempt” meant.

The 'Re-attempt' IE is currently defined in TS 29.002 is as follows.

> === Quotation from TS 29.002 ===
> 7.6.7.10 Re-attempt
> It indicates whether the failure occurred in a normal authentication attempt or in an authentication reattempt (there was a previous unsuccessful authentication).
> === Quotation end ===

Additionally, the related description in TS 33.102 is as follows.

> === Quotation from TS 33.102 ===
> 6.3.6 Reporting authentication failures from the SGSN/VLR to the HLR
>
> The purpose of this procedure is to provide a mechanism for reporting authentication failures from the serving environment back to the home environment.
> The procedure is shown in Figure 13.



VLR/SGSN
HLR
Authentication failure report
(IMSI, Failure cause, access type, authentication re-attempt,
VLR/SGSN address and RAND)

Figure 13: Reporting authentication failure from VLR/SGSN to HLR

The procedure is invoked by the serving network VLR/SGSN when the authentication procedure fails. The authentication failure report shall contain:

1. Subscriber identity;
2. Failure cause code. The possible failure causes are either that the network signature was wrong or that the user response was wrong;
3. Access type. This indicates the type of access that initiated the authentication procedure;
4. Authentication re-attempt. This indicates whether the failure was produced in a normal authentication attempt or it was due to an authentication reattempt (there was a previous unsuccessful authentication);
5. VLR/SGSN address;
6. RAND. This number uniquely identifies the specific AV that failed authentication.

The HE may decide to cancel the location of the user after receiving an authentication failure report and may store the received data so that further processing to detect possible fraud situations could be performed.
=== Quotation end ===

3. Discussion

Based on our analysis, the follows 4 cases could be a case where the 'Re-attempt' is set.

1) Authentication with (P-)TMSI failed in MS (reject cause 'MAC failure') and new authentication procedure (re-attempt) is taken because an IMSI obtained by the followed IDENTITY REQUEST procedure does not match to the original IMSI that linked with (P-)TMSI. See TS 24.008 section 4.3.2.6 c)

2) Authentication failed in MS (reject cause 'GSM authentication unacceptable') and new authentication procedure (re-attampt) is taken after MSC obtains UMTS authentication vectors from HLR. See TS 24.008 section 4.3.2.6 c)

3) Authentication failed in MS (reject cause 'synch failure') and new authentication procedure (re-attampt) is taken after MSC obtains new authentication vectors from HLR for re-synchronisation. See TS 24.008 section 4.3.2.6 c)

4) SRES mismatches with (P-)TMSI in VLR(SGSN) and new authentication procedure (re-attempt) is taken because an IMSI obtained by the followed IDENTITY REQUEST procedure does not match to the original IMSI that linked with (P-)TMSI. See TS 23.012 section 4.1.2.2 Procedure Authenticate_VLR, and TS 23.018 section 7.1.2.6 Procedure Authenticate_VLR

For 2) case, this is not a failure case since it may happen as the normal procedure especially along the GSM/UMTS broader. Therefore, CN4 consider that **the 'Re-attempt' parameter is set in the Authentication Failure Report Request message if the second authentication procedure is failed after the case 1), 3) or 4) procedure executed.**

4. Actions

To SA3 group.

ACTION: CN4 would like to ask following 2 questions in order for CN4 to put more clarity in TS 29.002 on use of ‘Re-attempt’ parameter. Moreover, if SA3 would conclude that TS 33.102 is also relevant to be put more clarity on use of ‘Re-attempt’ parameter, please update TS 33.102 and inform to CN4 so that CN4 could make an alignment with an update of TS 33.102.

Question 1: What is the purpose of the ‘Re-attempt’ parameter to be included in Authentication Failure Report Service? Particularly, how the HLR utilize this information.

Question 2: What is a situation where ‘Re-attempt’ parameter is set in VLR and SGSN.

5. Date of Next CN4 Meeting

CN4 #22	16th February – 20th February 2004, Atlanta, USA

3GPP TSG CN WG4 Meeting #21 *N4-031289*
Bangkok, Thailand, 27th – 31st October 2003

Title:	**LS on Special-RAND mechanism**
Response to:	S3-030653 (N4-031252) **LS on Special-RAND mechanism from SA3**
Release:	Rel-6
Source:	**CN4**
To:	**SA3**
Cc:	**CN1, GERAN2, T2**

Contact Person:

Name:	Ulrich Wiehe
Tel. Number:	+49 6621 169139
E-mail Address:	ulrich.wiehe@gksag.de

Attachments: **N4-031315 CR 29.002 (Rel-6) on addition of requestingPLMN-ID to Send Authentication Info Request**

1. Overall Description:

CN4 thank SA3 for their LS on Special RAND mechanism (S3-030653).
SA3's suggestion to extract the visited network identity from the lower layers of the MAP-stack i.e. from the SCCP calling party address of the request that arrives at the HLR/AuC and use it to determine uniquely the permitted algorithm settings was not over-enthusiastically well received by CN4. Although it may be possible as an implementation option to extract the needed information from the lower layer, CN4 do not endorse to mandate such behaviour.
As an alternative CN4 agreed to add the needed information (requesting PLMN-ID) as a parameter transferred on MAP level in the SendAuthenticationInfo request message. The CR introducing the new parameter in the MAP protocol is attached.

2. Actions:

none

3. Date of Next CN4 Meeting:

CN4 #22 16th February – 20 th February 2004; Atlanta, USA

3GPP TSG CN4 — CN4#21 **N4-031320**

27-31 Oct 2003, Bangkok, Thailand

Title:	LS on Clarification for the WLAN D’/Gr’ interface standardization
Release:	Rel-6
Work Item:	3GPP-WLAN interworking
Source:	CN4
To:	SA2
Cc:	

Contact Person:

Name:	Maria Carmen Belinchón
Represented company:	Ericsson
Tel. Number:	+34 91 339 3535
E-mail Address:	+34 91 339 2538

Attachments: None

1. Overall Description:

In CN4 there are ongoing discussions about the most suitable mechanisms to authorize, authenticate and retrieve user profile information through D’/Gr’ interface. This work has created confusion since it is not clear, according to stage 2 TS 23.234, whether this interface has to be defined in stage 3 by CN. The reasons for this lack of understanding are:

- The D’/Gr’ interface is defined in TS 23.234 as optional, and in annex A.3 is stated:

  > Since pre-R6 Subscriber Data records in HLR do not have any standardized information related to WLAN subscription, the choice and interpretation of the retrieved data is left up to the operator.

  With this statement, it seems that SA2 assumes that there will not exist any subscriber information in the HLR related to WLAN interworking, and the operator has to implement a proprietary solution to define such subscriber information and retrieve.

- The mechanism defined in annex 3 for subscriber profile retrieval (using MAP Restore Data) seems to contradict one of the main requirements of WLAN interworking, which is “This TS proposes solutions for operators who want to interwork their WLAN with an existing pre-R6 HLR/HSS” or “that the impacts in HLR/AuC shall be minimized”.

- If SA2 purpose was to have D’/Gr’ interface defined in stage 3 for R6, that seems to be the same case as for Wx interface, and then SA2 should clarify which of both interfaces wants to be defined by CN4 for this release (it does not make sense to (in the same release) define two protocols for the same purpose between two nodes).

- CN4 has also identified impacts on the HLR in the way it has to be upgraded to support D’/Gr’ interface.

2. Actions:

CN4 kindly request SA2 to reconsider whether D’/Gr’interface should be standardized having in mind that the existing HLR cannot be reused for these interfaces.

3. Date of Next CN4 Meeting:

CN4#22	February 2004	USA
CN4#23	May 2004	Croatia

3GPP TSG CN WG4 Meeting #21 Bangkok, Thailand, 27th – 31st October 2003

N4-031351

Title:	LS on identifying MMS Enabled devices and MMS Capabilities of those devices
Response to:	LS T2-030535 (N4-031242) on identifying MMS Enabled devices and MMS Capabilities of those devices from T2.
Release:	Rel-6
Work Item:	
Source:	CN4
To:	T2
Cc:	SA1, SA2

Contact Person:

Name:	Ulrich Wiehe
Tel. Number:	+49 6621 169139
E-mail Address:	ulrich.wiehe@gksag.de

Attachments:	N4-031328 (proposed revision of T2-030461.doc, CR 23.140 REL-6 on Legacy Terminal Detection)

1. Overall Description:

CN4 thank T2 for their LS on identifying MMS Enabled devices and MMS Capabilities of those devices.

CN4 would like to comment on the proposed CR attached to T2's LS (T2-030461) as follows:

The message flow providing an example for Legacy Terminal detection based on an IMEI query in Annex XX is base on standard MAP messages ATI (AnyTimeInterrogation) and PSI (ProvideSubscriberInfo). These messages can be used to retrieve the IMEI from the serving VLR or SGSN. It must be noted that by means of HLR configuration the MMSC address needs to be added to the HLR's internal table listing the nodes which are allowed to request information from the HLR with ATI. It must further be noted that the MAP messages ATI and PSI have originally been defined in the context of CAMEL. However, the subscriber addressed by the ATI and PSI messages is not required to subscribe to any CAMEL service.

CN4 have added comments to the CR 23.140 REL-6 on Legacy Terminal Detection. The commented revision is attached to this LS response.

Although the example mechanism specified in Annex XX is believed to be technically correct, CN4 identified the following deficiencies:

- the traffic load between MMSC, HLR, VLR/SGSN, and MS may increase significantly.
- it is not guaranteed that the retrieval of the IMEI by the MMSC is in all cases successful. If e.g. the serving VLR does not support PSI enhancements as specified for Rel-5, or the IMEI is not stored in the VLR and the MS is not reachable, the IMEI retrieval will be unsuccessful.
- Even if the IMEI could be successfully retrieved by the MMSC, the mapping onto terminal capabilities within the internal or external DB may be unsuccessful.

To this end CN4 makes no statement or recommendation as to the suitability of this solution over any other possible solutions.

2. Actions:

To T2

ACTION: T2 are asked to take the attached revised CR into consideration

3. Date of Next CN4 Meeting:

CN4 #22	16th February – 20 th February 2004	Atlanta, USA

3GPP TSG CN WG4 Meeting #21
Bangkok, Thailand, 27th – 31st October 2003

N4-031352

Title: LS on Change in MBMS Activation Procedure
Release: Release 6.
Work Item: MBMS

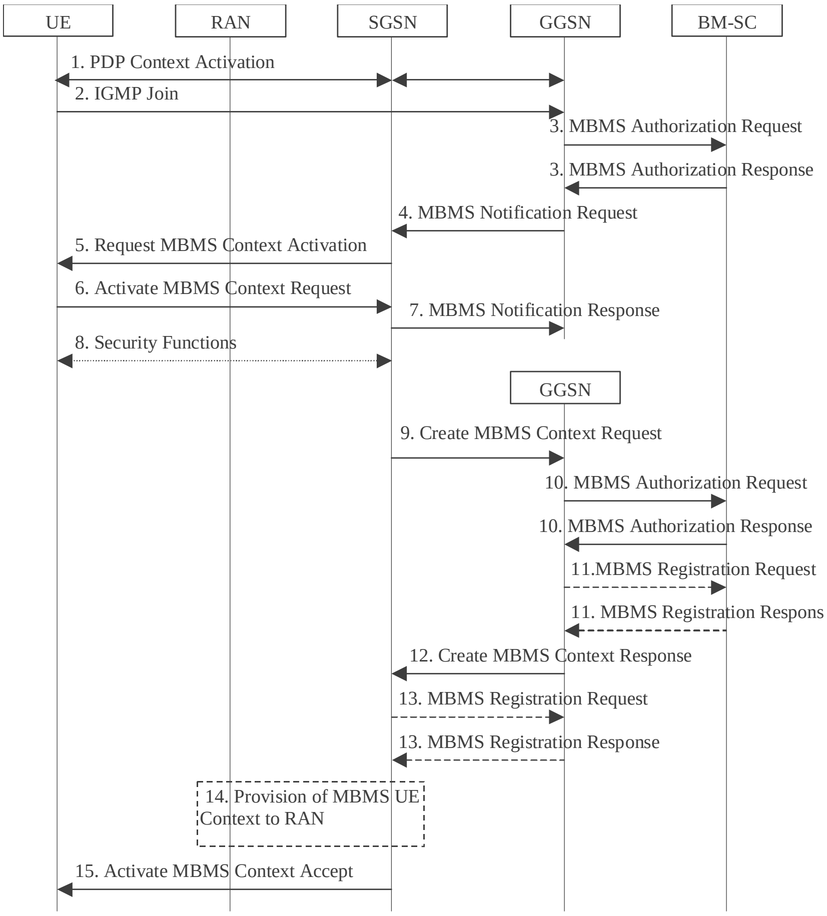
Source: CN4
To: SA2
Cc:

Contact Person:
Name: Hatef Yamini
Tel. Number: +44 7900823015
E-mail Address: Hatef.Yamini@three.co.uk

Attachments: None

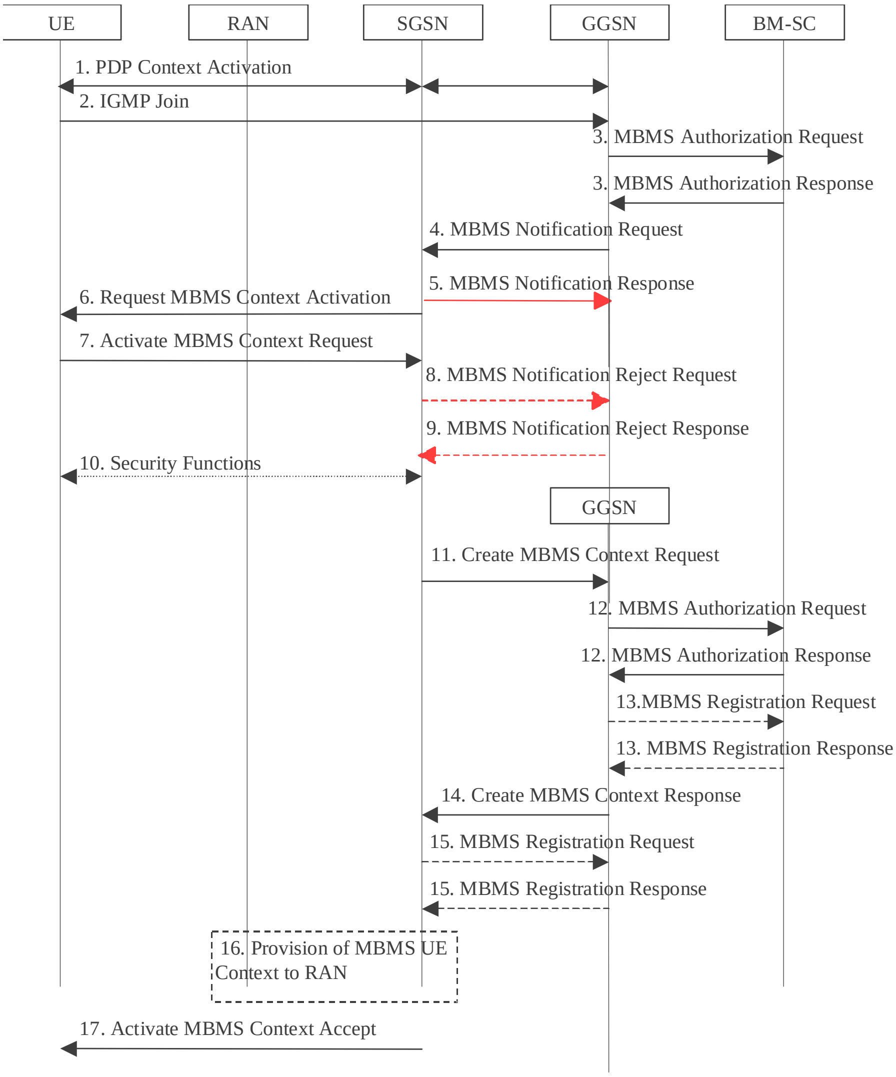
1. Overall Description:

CN4 have been working on the introduction of MBMS into GTP. During the course of the stage 3 design, it has been found necessary to slightly modify the stage 2 flow in order to meet the requirements of GTP with relation to GTP timers.
The stage 2 flow is copied below for information.


UE
RAN
SGSN
GGSN
BM-SC
1. PDP Context Activation
2. IGMP Join
3. MBMS Authorization Request
3. MBMS Authorization Response
4. MBMS Notification Request
5. Request MBMS Context Activation
6. Activate MBMS Context Request
7. MBMS Notification Response
8. Security Functions
GGSN
9. Create MBMS Context Request
10. MBMS Authorization Request
10. MBMS Authorization Response
11.MBMS Registration Request
11. MBMS Registration Respons
12. Create MBMS Context Response
13. MBMS Registration Request
13. MBMS Registration Response
14. Provision of MBMS UE Context to RAN
15. Activate MBMS Context Accept

During Step 4, a GTP MBMS Notification Request message shall be sent by the GGSN towards the SGSN. The GTP response message, the MBMS Notification Response, is then sent during step 7 indicating "*successful or unsuccessful MBMS context activation for the reason of SGSN or UE*" as stated in TS23.246.

CN4 are concerned that during this time, GTP retry timers may time out causing possible errors within the Gn interface. In order to address this, an immediate response to the MBMS Notification Request (step 4 above) shall be sent, indicating that the SGSN has understood the request, and is processing the message. In the case of explicit reject of the network initiated MBMS context activation by the UE, or loss of radio contact with the UE, two new messages have been defined to indicate the failure of the MBMS context activation; The MBMS Notification Reject Request / MBMS Notification Reject Response. These messages now serve the purpose of the MBMS Notification Response message (step 7 above). Additionally, it should be noted that this procedure is also in line with the existing method for "regular" network initiated PDP context activation. The updated flow is shown below with the modified messages shown in red;


UE
RAN
SGSN
GGSN
BM-SC
1. PDP Context Activation
2. IGMP Join
3. MBMS Authorization Request
3. MBMS Authorization Response
4. MBMS Notification Request
5. MBMS Notification Response
6. Request MBMS Context Activation
7. Activate MBMS Context Request
8. MBMS Notification Reject Request
9. MBMS Notification Reject Response
10. Security Functions
GGSN
11. Create MBMS Context Request
12. MBMS Authorization Request
12. MBMS Authorization Response
13.MBMS Registration Request
13. MBMS Registration Response
14. Create MBMS Context Response
15. MBMS Registration Request
15. MBMS Registration Response
16. Provision of MBMS UE Context to RAN
17. Activate MBMS Context Accept

CN4 believe that all the required functionality from the stage 2 specifications shall be delivered by this stage 3 design, and furthermore, will alleviate the problem encountered within the protocol design for MBMS GTP messages.

2. Actions:

To SA2 group.

ACTION: CN4 asks SA2 to consider the impact of the change, and guide CN4 if an adverse impact is seen from this change.

3. Date of Next CN4 Meeting:

CN4 #22	16 February - 20 February 2004	USA
CN4 #23	10 May - 14 May 2004	Zagreb, Croatia

3GPP TSG CN WG4 Meeting #21 ***N4-031367***
Bangkok, Thailand, 27th – 31st October 2003

Title: LS on DNS top level domains
Release: Release 5
Work Item: IMS

Source: CN4
To: GSMA IREG PACKET
Cc: TSG-CN

Contact Person:
Name: Stephen Hayes
Tel. Number: +1 4693608500
E-mail Address: stephen.hayes@ericsson.com

Attachments: None

---

1. Overall Description:

CN4 thanks GSM IREG PACKET for the rapid response on the issue of using the ".gprs" TLD for IMS. CN4 appreciates that the introduction of ".3gppnetwork.org" will add additional administrative overhead in the GRX

However, given that:
- Release 5 is frozen and changes should be made only due to major faults being found,
- the currently specified usage of ".3gppnetwork.org" is technically viable,
- the IETF is the organization responsible for standardized DNS policy,

3GPP is reluctant to change what is currently specified.

The IETF has explicitly requested that 3GPP NOT further extend the use of the ".gprs" domain. The use of unregistered TLDs (even in private networks) is a very high profile issue within the IETF. Violation of this agreement would likely have political ramifications on the 3GPP/IETF working relationship.

3GPP realizes that the incremental increase in usage of ".gprs" is minor (only used for initial IMS registrations when no ISIM is present). It is possible that the IETF would be willing to withdraw its objections if they appreciated the limited situation being addressed. The CR changing the TLD from ".3gppnetwork.org" to ".gprs" will be progressed to CN#22. If the GSMA can persuade the IETF that use of ".gprs" is acceptable in this limited case, then this CR can likely be approved. If not, the CR will likely be rejected.

2. Actions:

To GSM IREG.

ACTION: Initiate discussions with IETF on granting an exception for the use of ".gprs" in the case of initial IMS registrations when no ISIM is present. Thomas Narten (Area Director, Internet Area) is the appropriate contact point within the IETF for this issue.

3. Dates of Next TSG-CN/CN4 Meetings:

TSG-CN #22	10 December - 12 December 2003	Hawaii, USA
CN4 #22	16 February - 20 February 2004	Atlanta, USA

3GPP TSG CN WG4 Meeting #21 Bangkok, Thailand, 27th – 31st October 2003

N4-031387

Title:	**LS Reply on "Trace Management"**
Response to:	**LS (S5-038444) on Rel-6 Subscriber and Equipment Trace impacts to the Core Network from WG SA5**
Release:	**Release 6**
Work Item:	**OAM-Trace**
Source:	**CN4**
To:	**SA5**
Cc:	**CN1, CN2**

Contact Person:

Name:	**Jari Jansson**
Tel. Number:	**+385 40 5550719**
E-mail Address:	jari.jansson@nokia.com

Attachments: None

1. Overall Description:

CN4 thanks SA5 on their liaison statement concerning the Subscriber and Equipment Trace impacts.

CN4 has investigated the technical questions included in the liaison statement and would like to give following answers:

1. *Study the possibility of creation of a new Trace Session activation message (or modification of an existing message for this purpose) according to the needs of SA5 SWG-D between the following Network Elements:*
   - i. *HSS and MSS*
   - ii. *HSS and SGSN*
   - iii. *HSS and S-CSCF*
   - iv. *SGSN and GGSN*
   - v. *MSS and MGW*

For two first interfaces the understanding of CN4 is that existing MAP services can be modified to cover the new requirements.

For the third interface the understanding of CN4 is that new messages need to be defined to the Cx protocol.

For the fourth interface the understanding of CN4 is that existing GTP services can be modified to cover the requirements. However the support of different depths of trace measurement is something that CN4 has not studied.

For the fifth interface CN4 has not concluded due to lack of availability of stage 2 specification, however contribution has been received proposing that a new package needs to be defined to the Mc protocol, but decision on this has been postponed.

2. *Study the start triggering event parameter and provide an answer whether the Subscriber identity (IMSI) and MS identity (IMEI(SV)) is available for the start triggering events (see the tables above for the events and corresponding signalling messages).*

For MSC Server, SGSN and GGSN the understanding of CN4 is that IMSI is available for the events listed, but not for MGW. IMEI(SV) is not necessarily available in MSC Server, SGSN, GGSN or MGW. Also the understanding of CN4 is that the start triggering events listed are the first messages of the transactions traced.

Only exception is the handover, where the start message for handover is BSSMAP-HANDOVER-REQUIRED or RANAP-RELOCATION-REQUIRED. However if the meaning is to use the first message from the target side of the handover as the start triggering event then the understanding of CN4 is that the messages listed can be used for handover.

3. *Study the stop triggering event parameter and provide an answer whether the listed signalling messages are the last messages in the transaction of events listed above.*

CN4 has not been able to reach a conclusion on this as some members of CN4 wished to consider this in conjunction with the detailed trace requirements. We hope to be able to answer this after next CN4 meeting.

4. *Reply to SA5 SWG-D whether CN4 can provide a solution and if so, give SA5 SWG-D the CN4 view of the solution and an indication of the time required to provide such a solution.*

To be able to make the needed modifications CN4 would need the stage 2 specification (32.422) to be available and stable. CN4 decided that new WID for CN changes is required in order to provide clarity on the required CN changes due to the relative large amount of nodes and interfaces that may be affected and the specific requirements for these nodes and currently the SA WID does not include enough detail for the CN stage 3 work. This would be a CN4 owned WID but include other CN impacts and thus address the concern from CN1 via previous LS discussions. The current understanding of CN4 is that at least the MAP, GTP and Mc protocol changes can be done within Rel-6 timeframe with the condition that there exists the 32.422 specification before next CN4 meeting in February 2004.

One specific question that needs clarification is that in the list of interfaces there is CAP protocol listed for SGSN (but not for MSC Server). There does not seem to however be any triggering events for CAP protocol listed. CN4 would like to ask clarification from SA5 about the need to trace CAP protocol and also to inform that if CAP protocol needs to be traced then CN2 as a responsible group for CAP protocol would need to be involved in the discussions.

2. Actions:

To SA5 group.

ACTION: CN4 asks SA5 group to:

1. Study the answers given by CN4 and give further comments regarding them.
2. Clarify the availability of 32.422 specification.
3. Give guidance for the need of traceability of CAP protocol and if such a need exists indicate that to CN2 group.

3. Date of Next CN4 Meeting:

CN4 #22	16th February – 20th February 2004