**3GPP TSG CN Plenary Meeting #22** **NP-030472**
**10th - 12th December 2003. Hawaii, USA.**

**Source:** **MCC**

**Title:** **All LSs sent from CN1 since TSG CN#21 meeting**

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

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

**Introduction:**

This document contains **8 agreed** LSs sent from **TSG CN WG1#32**, and are forwarded to TSG CN Plenary meeting #21 for information only.

| Meeting | Type | TDoc # | Status | Source | Tdoc Title | Comments |
|---|---|---|---|---|---|---|
| N1-32 | LS OUT | N1-031606 | AGREED | Richard/Samsung | Handling of MBMS UEs in RRC-connected, PMM-IDLE state | Reply to 1409.<br>To: RAN2,<br>Cc: SA2, RAN3 |
| N1-32 | LS OUT | N1-031607 | AGREED | Georg/Nokia | Response to LS “Nature of SIP Signalling” | Reply to 1412.<br>To: RAN3,<br>Cc: RAN2 |
| N1-32 | LS OUT | N1-031610 | AGREED | Gabor/Nokia | LS Reply on “Trace Management” | Reply to 1420.<br>To: SA5,<br>Cc: CN4 |
| N1-32 | LS OUT | N1-031612 | AGREED | Robert/Siemens | Reply LS on Special-RAND mechanism | Reply to 1462.<br>To: SA3,<br>Cc: GERAN2 |
| N1-32 | LS OUT | N1-031690 | AGREED | Christian/Ericsson | LS on WLAN requirements | To: SA1, SA2,<br>Cc: T3 |
| N1-32 | LS OUT | N1-031724 | AGREED | Gabor/Nokia | The requirement and feasibility of IMS watcher authentication | Reply to 1464.<br>To: SA3,<br>Cc: SA1, SA2 |
| N1-32 | LS OUT | N1-031725 | AGREED | Georg/Nokia | LS “Questions on the possibility to not use Preconditions in Release 5” | Related to 1455, 1538, 1549,<br>To: SA2,<br>Cc:<br>Revised from 1644 |
| N1-32 | LS OUT | N1-031728 | AGREED | Keith/Lucent | LS on Introducing the Privacy Mechanism in Stage 2 | Reply to 1461.<br>To: SA3,<br>Cc: SA2.<br>Revised from 1611. |

# 3GPP TSG-CN1 Meeting #32 Tdoc N1-031606
# Bangkok, Thailand, 27 – 31 October 2003

|  |  |
|---|---|
| **Title:** | Handling of MBMS UEs in RRC-connected, PMM-IDLE state |
| **Response to:** | LS (**R2-032282**) on Handling of MBMS UEs in RRC-connected, PMM-IDLE state from RAN2 |
| **Release:** | Released 6 |
| **Work Item:** | MBMS |
| **Source:** | CN1 |
| **To:** | RAN2 |
| **Cc:** | SA2, RAN3 |

**Contact Person:**

|  |  |
|---|---|
| **Name:** | Richard Brook |
| **Tel. Number:** | +44 7776 181555 |
| **E-mail Address:** | Richard,Brook@samsung.com |

**Attachments:**

### 1. Overall Description:

CN1 thanks RAN 2 for their LS on Handling of MBMS UEs in RRC-connected, PMM-IDLE state.

CN1 have briefly discussed the question raised by RAN2 and are currently thinking of using the Service Request procedure to handle this, but that some changes to this procedure maybe required.
This is currently under investigation.

### 2. Actions:

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

|  |  |  |
|---|---|---|
| CN1_33 | 16th – 20th February 2004 | TBD, USA (NA friends of 3GPP) |
| CN1_34 | 10th – 14st May 2004 | TBD, Croatia (EF3) |

**3GPP TSG CN1#32 meeting** **N1-031607**
**Bangkok, Thailand, October 27-31, 2003**

**Title:** **Response to LS "Nature of SIP Signalling"**
**Release:** Release 6

**Source:** CN1
**To:** RAN3
**Cc:** RAN2

**Contact Person:**
**Name:** Georg Mayer
**Tel:** +358 50 48 21 43 7
**E-mail :** georg.mayer@nokia.com

**Attachments:** None

### 1. Overall Description:

The RAN3 LS on "Nature of SIP signalling" was discussed in CN1#32 meeting.

Currently, a dedicated PDP context with possible QoS optimisations is used to carry IMS specific SIP, DHCP and DNS signalling. The nature of SIP signalling, i.e. whether a certain signalling element is related to call control or not, cannot be determined within that dedicated PDP context, as

- a straightforward mapping from message type to applications is not possible. For example a NOTIFY request can carry information related to the presence service as well as call control related information (e.g. a users registration status).

- those messages, which carry call control related information (e.g. INVITE), may include headers or bodies with additional, non call control information. This additional information may be much larger than the rest of the message (e.g. an INVITE body may include a picture of the caller)

- those headers which include call control related information (e.g. Route), may include additional parameters with additional, non call control information.

Due to varying nature of Signalling, the feasible solution to differentiate signalling traffic at the radio bearer level is very difficult to define. Thus CN1 would like to inform RAN3 that no extra information in addition to the Signalling indication flag / QoS flag could be sent to UTRAN during Signalling RAB set-up in R6 time frame.

### 2. Actions

None

### 3. Date of Next TSG CN1 meeting

## 3GPP TSG-CN1 Meeting #32 *Tdoc N1-031610*
## Bangkok, Thailand, 27-31 October

|  |  |
|---|---|
| **Title:** | LS Reply on "Trace Management" |
| **Response to:** | N1-031420 (S5-032644) |
| **Release:** | REL-6 |
| **Source:** | CN1 |
| **To:** | SA5 |
| **Cc:** | CN4 |

**Contact Person:**

|  |  |
|---|---|
| **Name:** | Gábor Bajkó |
| **Tel. Number:** | tel:+36 20 9849259 |
| **E-mail Address:** | Gabor.Bajko@nokia.com |

**Attachments:** None

### 1. Overall Description:

CN1 thanks for SA5 for the clarifications provided regarding the trace requirements; CN1 will take these into consideration when it starts the work on trace activation.

CN1 can confirm that IMEI and IMEISV are not available in the CSCFs.

### 2. Actions: none

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

|  |  |  |
|---|---|---|
| CN1_33 | 16th – 20th February 2004 | TBD, USA (NA friends of 3GPP) |
| CN1_34 | 10th – 14st May 2004 | TBD, Croatia (EF3) |

# 3GPP TSG-CN1 Meeting #32 Tdoc N1-031612
# Bangkok, Thailand, 27 – 31 October 2003

**Title:** Reply LS on Special-RAND mechanism

**Response to:** LS (S3-030652 / N1-031462) from SA3 on Special-RAND mechanism

**Release:** Rel-6

**Source:** CN1

**To:** SA3

**Cc:** GERAN 2

**Contact Person:**
**Name:** Robert Zaus
**Tel. Number:** +49 89 63675206
**E-mail Address:** robert.zaus@siemens.com

**Attachments:** ---

---

**1. Overall Description:**

CN1 would like to thank SA3 for their LS on the Special-RAND mechanism.

CN1 briefly discussed the proposed special-RAND mechanism described in clause 2 of Tdoc S3-030651and agreed that it looks feasible.

Furthermore, CN1 would like to comment on the analysis in subclause 3.2.2 of the same document:

> 3.2.2 GSM packet switched
>
> It should be considered what happens when a Special RAND capable mobile receives an AUTHENTICATION AND CIPHERING REQUEST instructing it to start ciphering using an algorithm that is forbidden to be used with the current cipher key. It is proposed that the GMM layer in the mobile treats this as an error case and does not start ciphering uplink traffic at the LLC layer [24.008, 43.020]. Since the SGSN is expecting uplink traffic to be encrypted it will result in a layer 2 failure in the SGSN.
>
> In summary no special error handling needs to be specified.

and to ask SA3 for guidance on the following issues:

1) On the Gb interface it is possible to perform authentication and start ciphering with one procedure, by including both a RAND and an appropriate ciphering algorithm in the AUTHENTICATION AND CIPHERING REQUEST message.

   If the authentication challenge is a UMTS authentication and the message contains:
   - both an authentication failure (MAC failure or Synch failure) and
   - a ciphering algorithm that is not permitted according to the special-RAND information,

   which error takes precedence? Should the UE report an Authentication and Ciphering Failure to the network or should it diagnose a 'not permitted ciphering algorithm' first and skip the authentication?

2) If the GMM layer in the UE is required to treat the request for a 'not permitted ciphering algorithm' as an error, the UE should not return an AUTHENTICATION AND CIPHERING RESPONSE message. According to TS 24.008 (subclause 4.7.7.3), however, without receipt of an AUTHENTICATION AND CIPHERING RESPONSE message the SGSN will not start ciphering. I.e. the layer 2 failure mentioned in the above scenario will not occur.

   CN1 noted that possible candidates for an explicit error indication by the UE to the SGSN would be the GMM STATUS or the AUTHENTICATION AND CIPHERING FAILURE message, but did not discuss this in detail.

3) When it is proposed that the UE shall not start ciphering the uplink traffic at the LLC layer, what kind of traffic is the UE allowed to send in the uplink – signalling and/or user data, or none at all?

4) Finally, what is the expected UE reaction after detection of a 'not permitted ciphering algorithm' error?
    - Bar the cell, as in the case the network fails a UMTS authentication procedure (TS 24.008, subclause 4.7.7.6.1)?
    - Deactivate all active PDP contexts?
    - Perform a detach from the network?
    - Or any combination of these measures?

## 2. Actions:

**To SA3 group.**

**ACTION:** CN1 kindly asks SA3 to provide answers to the above questions so that CN1 can get a better understanding of the requirements.

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

| | | |
|---|---|---|
| CN1_33 | 16th – 20th February 2004 | Atlanta, USA (NA friends of 3GPP) |
| CN1_34 | 10th – 14st May 2004 | TBD, Croatia (EF3) |

**3GPP TSG-CN1 Meeting #32 Tdoc N1-031690**
**Bangkok, Thailand, 27 – 31 October 2003**

| | |
|---|---|
| **Title:** | LS on WLAN requirements |
| **Release:** | Rel-6 |
| **Work Item:** | WLAN Interworking |
| **Source:** | CN1 |
| **To:** | SA1, SA2 |
| **Cc:** | T3 |

**Contact Person:**
**Name:** Christian Herrero
**Tel. Number:** +46 46 231812
**E-mail Address:** christian.herrero@ericsson.com

**1. Overall Description:**

At CN1#32, CN1 has investigated under the work item WLAN Interworking the following items:

1. Terminology for the WLAN access network selection procedure:
Two different proposals have been evaluated in order to define at stage 3 the WLAN access network selection (i.e. WLAN radio network selection) as defined in 3GPP TS 22.011, 3GPP TS 22.011 and 3GPP TS 23.234.

    - **WLAN selection**: Procedure for the selection among the available WLANs.
    - **I-WLAN selection**: Selection among the available I-WLANs.

CN1 has agreed the working assumption of using the term 'WLAN selection', due to the following reasons:

- The term WLAN selection has no restriction to the interworking WLAN's and therefore WLAN as such is correct for the case used at stage 3,
- and WLAN PLMN selection is performed only amongst the interworking PLMNs.

During the terminology discussion at CN1, it was pointed out that 'I-WLAN selection' is the appropriate term used by the stage 1 specifications (e.g. 3GPP TS 22.101 and 3GPP TS 22.011). However, it was also pointed out that 3GPP TS 22.011 when referring to network selection states in subclause 6.1 that "The UE shall select between multiple WLANs'"**.**

CN1 would like to check whether the working assumption on terminology for WLAN access selection is correct.

2. The Manual and Automatic mode of WLAN access network selection:
The current text in subclause 6.1 of 3GPP TS 22.011 states "*The UE shall support both manual and automatic network selection mechanisms (modes) as standardized. The UE shall use the last network selection mode used, as the default mode, at every switch-on. The user shall be given the opportunity to change the network selection mode at any time*".

The CN1 discussed that two new modes for WLAN access network selection seemed to be needed, but CN1 could not completely agree whether this is a requirement at stage 1 or not. Thus, CN1 would like to check whether new Manual and Automatic network selection modes shall be supported for WLAN access network selection (i.e WLAN radio network selection).

3. Ways to indicate operator and user preferences:
The current text in the subclause 6.1 of 3GPP TS 22.011 states "*When selecting a PLMN that is accessed via an interworked WLAN, this selection shall be based on operator and end user preferences. This set of preferences may be different from the preferences used for direct 3GPP access. The UE shall select between multiple WLANs in the same coverage area based on the operator preferences and user preferences by using similar procedures as for Network Selection without WLAN Interworking*".

CN1 has discussed a possible way to indicate operator and user preferences to fulfil the subclause 6.1 of 3GPP TS 22.011by the usage of the following lists in order to perform WLAN access network selection and WLAN PLMN selection:

- For WLAN access network selection (Case of IEEE 802.11 WLANs); ‘User preferred SSID list’, ‘Operator preferred SSID list’.
- For WLAN PLMN selection; ‘User Controlled PLMN Selector for WLAN access’, ‘Operator Controlled PLMN Selector for WLAN access’. Another list, which may contain a list of PLMN codes to which the WLAN UE called ‘Forbidden PLMNs for WLAN access’, might be used to not attempt to authenticate to an available PLMN code.

CN1 has also discussed that the above lists should be stored in the WLAN UE as one way to indicate operator and user preferences, but it is questioned whether the lists shall be stored in the ME or USIM (part of the WLAN UE), because the text in subclause 13.1.1 of 3GPP TS 22.101 indicates, “*Access via a I-WLAN shall be possible using earlier releases (than the current release) of the UICC or using a SIM*”.

4. <u>Broadcast of the VPLMN ID in the SSID</u>:
3GPP TS 23.234 in subclause 5.4.3 seems to indicate that a VPLMN advertisement should be supported by WLAN, but CN1 could not agree whether the broadcast of the VPLMN in the SSID is a requirement at stage 2 or not. So, CN1 would like to check whether the broadcast of the VPLMN in the SSID is a requirement at stage 2 or not.

5. <u>The need of I-WLAN SSID</u>:
According to 3GPP TS 23.234 (subclause 5.4.2.1) it seems possible to indicate the support of an I-WLAN SSID value by the WLAN. Subclause 5.4.2.1 also states that this value shall be defined in the appropriate stage 3 specification.
CN1 would kindly like to ask whether a common I-WLAN SSID is needed.

**2. Actions:**

**To SA1:**

CN1 kindly asks SA1 to consider the comments given above, and to address the questions asked by CN1 in the bullet items 1, 2, and 3 in order to check whether the working assumptions and discussions made by CN1 are capable of satisfying the existing stage 1 requirements.

**To SA2:**

CN1 kindly asks SA2 to consider the comments given above, and to address the questions asked by CN1 in the bullet items 1, 4 and 5 in order to check whether the working assumptions and discussions made by CN1 are capable of satisfying the existing stage 2 requirements.

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

| | | |
|---|---|---|
| CN1_33 | 16th – 20th February 2004 | TBD, USA (NA friends of 3GPP) |
| CN1_34 | 10th – 14st May 2004 | TBD, Croatia (EF3) |

**3GPP TSG-CN1 Meeting #32** ***Tdoc N1-031724***
**Bangkok, Thailand, 27-31 October**

| | |
|---|---|
| **Title:** | **The requirement and feasibility of IMS watcher authentication** |
| **Response to:** | N1-031464 (S3-030654) |
| **Release:** | REL-6 |
| | |
| **Source:** | CN1 |
| **To:** | SA3 |
| **Cc:** | SA1, SA2 |

**Contact Person:**

**Name:** Gábor Bajkó
**Tel. Number:** tel:+36 20 9849259
**E-mail Address:** Gabor.Bajko@nokia.com

**Attachments:** None

### 1. Overall Description:

CN1 thanks SA3 for the liaison statement regarding the requirement and feasibility of IMS watcher authentication.

CN1 has investigated the need for any watchers to be authenticated at the presence server in the IMS, and came to the following conclusion:

- For a watcher attached to and authenticated in IMS, the P-Asserted-Identity header is there in all requests, which uniquely identifies the originator of the request. Requesting the watcher to authenticate in addition would not bring any further security in the system. If some IMS service would need such an extra authentication for any reason, that is not prohibited but the ways how to do it should be outside of scope of 3GPP.

- Non-IMS watchers or watchers accessing the Presence information from a non-trusted IMS, would not have any P-Asserted-Identity in the request, thus their identity would not be known. Some mechanism to authenticate these watchers might be needed, but the exact mechanism is left to SA3 to decide on.

### 2. Actions:

**To SA1 and SA2: none.**

**To SA3 group.**

**ACTION:** SA3 is asked to take into consideration the analysis made above.

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

| | | |
|---|---|---|
| CN1_33 | 16th – 20th February 2004 | TBD, USA (NA friends of 3GPP) |
| CN1_34 | 10th – 14st May 2004 | TBD, Croatia (EF3) |

**3GPP TSG CN1#32 meeting** **N1-031725**
**Bangkok, Thailand, October 27-31, 2003**

**Title:** **LS on "Questions on the possibility to not use Preconditions in Release 5"**

**Release:** Release 5

**Source:** CN1

**To:** SA2

**Contact Person:**
**Name:** Georg Mayer
**Tel:** +358 50 48 21 43 7
**E-mail :** georg.mayer@nokia.com

**Attachments:** None

---

**1. Overall Description:**

In the Release-5 version of 24.229 it is currently stated that, when the UE receives an indication that the remote side does not support the SIP preconditions extension, it shall not try to establish the related session (i.e. shall not send out another INVITE without preconditions to the remote end). The call simply fails. Moreover, no error behaviour is defined on the network side for the case a misbehaving UE sends an INVITE without preconditions.

This needs to be changed based on a recent decision from SA2 (CR337rev2 on TS23.228 Release 5). During CN1#32 different contributions addressed the problem in different ways and no common opinion could be reached in CN1. During the related discussion it became clear that CN1 needs further guidance on the related stage 2 requirement.

In parallel to this, a solution for Release-6 was proposed but could not be agreed during CN1#32.. This is needed due to interworking with non-IMS networks (under Release 6 work item).

For Release-5 several possible solutions were discussed. The following list shows four possible ways forward, but other combinations are also possible:

1) **Adoption of Release-6 changes already in Release-5**
This solution will have include the following:
- UE may send INVITE requests without preconditions
- Network enabled for handling for sessions established without preconditions, which may have impact oncharging and Go related procedures.
- CSCFs can be configured to reject INVITE requests that do not include preconditions

In this case the Release-5 solution will be delayed until the Release-6 solution has been agreed in CN1#32.

This change would introduce IMS / SIP interworking already in Release-5.

2) **UE may send INVITE without preconditions, but Rel-5 network does reject all such INVITE requests, i.e.:**
- UE may send INVITE requests without preconditions
- CSCFs can be configured to reject INVITE requests that do not include preconditions

The UE would be able to send INVITE requests without preconditions only when attached to a

Rel-6 IMS network.

A Rel-6 UE attached to a Rel-5 network would not be able to establish a call to another UE that does not support preconditions. If the same UE would be attached to a Rel-6 IMS, this would work.

Some delegates were concerned that this solution would close the door for the introduction of services to Release-5 which do not require the support of preconditions.

If this solution is chosen it still needs to be decided whether the rejection of INVITE requests without preconditions is mandatory to be done by the Rel-5 network or optional.

3) **UE does not send INVITE requests without precondition, but network is able to handle such INVITE requests, i.e.**
   - Network enabled for handling for sessions established without preconditions, which may have impact oncharging and Go related procedures.
   - CSCFs can be configured to reject INVITE requests that do not include preconditions

   In this case a Rel-6 UE could roam to a Rel-5 network and still would be able to send INVITE requests without precondition. The Rel-5 UE on the other hand would not be able to send INVITE requests without precondtions, even if the network would support this. This alternative does not seem to be aligned with the already approved stage 2 design.

4) **No change to the existing 24.229 procedures**, i.e. the Rel-5 UE and network would not support any mechanisms for session establishment without preconditions. The network would not explicitly block such attempts. However, this alternative does not seem to be aligned with the already approved stage 2 design.

   In this case a Rel-6 UE roaming to a Rel-5 would be able to send INVITE without preconditions into a Rel-5 network, which would then not be able to handle it. Impacts were identified in TR 29.962.

### 2. Actions

CN1 kindly asks SA2 to study the above cases and give further guidance and clarifications on the related requirement back to CN1.

### 3. Date of Next TSG CN1 meeting

| | |
|---|---|
| TSG CN WG1 #33 | 16-20 February, USA |

# 3GPP TSG-CN1 Meeting #32 Tdoc N1-031728
# Bangkok, Thailand, 27 – 31 October 2003

| | |
|---|---|
| **Title:** | LS on Introducing the Privacy Mechanism in Stage 2 |
| **Response to:** | LS (S3-030649) on Introducing the Privacy Mechanism in Stage 2 from WG SA3 |
| **Source:** | **CN1** |
| **To:** | **SA3** |
| **Cc:** | **SA2** |

**Contact Person:**

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

**Attachments:** None

### 1. Overall Description:

WG CN1 thanks WG SA3 for their liaison in S3-030649.

WG CN1 would like to clarify the appropriate IETF references made in the proposed CR.

RFC 3323 specifies the essential capabilities of the privacy function, and specifies a number of optional privacy capabilities, i.e. header (RFC 3323 subclause 5.1), session (RFC 3323 subclause 5.2) and user (RFC 3323 subclause 5.3). None of these options are currently specified in 3GPP TS 24.229, and the complete implementation of these options cannot occur with SIP proxy capabilities.

The essential capabilities of the privacy function can be regarded as:

- the definition of the privacy header and its syntax
- the operation of the "none" value such that the user requests that a privacy service apply no privacy functions to this message, regardless of any pre-provisioned profile for the user or default behavior of the service. User agents can specify this option when they are forced to route a message through a privacy service which will, if no Privacy header is present, apply some privacy functions which the user does not desire for this message. Intermediaries MUST NOT remove or alter a Privacy header whose priv-value is 'none'. User agents MUST NOT populate any other priv-values (including 'critical') in a Privacy header that contains a value of 'none'.
- the operation of the "critical" value such that the user asserts that the privacy services requested for this message are critical, and that therefore, if these privacy services cannot be provided by the network, this request should be rejected. Criticality cannot be managed appropriately for responses.

RFC 3325 (in addition to defining the P-Asserted-Identity header and the P-Preferred-Identity header, defines the privacy option "id" that is currently specified within 3GPP TS 24.229.

Any specification of the privacy capability therefore requires references to both RFC 3323 (for the coding of the header and the operation of "none" and "critical") and RFC 3325 (for the operation of the "id" privacy option.

### 2. Actions:

**To WG SA3 group.**

**ACTION: WG CN1 asks WG SA3 to revise the CR to make the appropriate references to RFCs as indicated by the discussion above.**

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

| | | |
|---|---|---|
| CN1_33 | 16th – 20th February 2004 | TBD, USA (NA friends of 3GPP) |

| | | |
|---|---|---|
| CN1_34 | 10th – 14st May 2004 | TBD, Croatia (EF3) |