

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246 CR 014** ⌘ rev **-** ⌘ Current version: **6.0.0** ⌘

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

Proposed change affects: | UICC apps ME Radio Access Network Core Network

| | | | |
|------------------------|---|-----------------|---|
| Title: | ⌘ Protection of the Gmb reference point | | |
| Source: | ⌘ Siemens | | |
| Work item code: | ⌘ MBMS | Date: | ⌘ 27/09/2004 |
| Category: | ⌘ C | Release: | ⌘ Rel-6 |
| | Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | Use <u>one</u> of the following releases: Ph2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6) Rel-7 (Release 7) |

| | |
|--------------------------------------|--|
| Reason for change: | ⌘ The DIAMETER protocol has been specified within TS 29.061 for use on the Gmb reference point. Since DIAMETER runs over IP and since the Gmb reference point (GGSN - BM-SC or GGSN - Gmb proxy - BM-SC) always resides within an operator's network, NDS/IP protection may be used (TS 33.210) according to Za or Zb reference points. |
| Summary of change: | ⌘ Removal of the Editor's Note that the Gmb reference point security is for ffs. Add NOTE that NDS/IP mechanism may be used for securing the Gmb reference point. |
| Consequences if not approved: | ⌘ Gmb reference point protection remains unspecified |

| | | | | | | | |
|------------------------------|---|---|---|--------------------------|-------------------------------------|--|--|
| Clauses affected: | ⌘ 2, Annex C | | | | | | |
| Other specs affected: | <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications ⌘ | Y | N | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| Y | N | | | | | | |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | | | | | | |
| | <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">N</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications | N | N | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| N | N | | | | | | |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | | | | | | |
| | <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">N</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications | N | N | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | |
| N | N | | | | | | |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | | | | | | |
| Other comments: | ⌘ | | | | | | |

===== BEGIN CHANGE =====

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".
- [3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".
- [4] 3GPP TS 33.102: "3G Security; Security Architecture".
- [5] 3GPP TS 22.246: "MBMS User Services".
- [6] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".
- [7] 3GPP TS 31.102: "Characteristics of the USIM application".
- [8] IETF RFC 2617 "HTTP Digest Authentication".
- [9] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"
- [10] IETF RFC 1982 "Serial Number Arithmetic".
- [11] IETF RFC 3711 "Secure Real-time Transport Protocol".
- [12] 3GPP TS 43.020: "Security related network functions".
- [13] [3GPP TS 33.210: "Network domain security; IP network layer security"](#).

===== END CHANGE =====

===== BEGIN NEXT CHANGE =====

Annex C (normative): Multicast security requirements

C.1 Requirements on security service access

C.1.1 Requirements on secure service access

- R1a: A valid USIM shall be required to access MBMS User Services.
- R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS User Services by masquerading as authorized users.

C.1.2 Requirements on secure service provision

- R2a: It shall be possible for the network (e.g. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS User Services.
- R2b: It shall be possible to prevent the use of a particular USIM to access MBMS User Services.
- NOTE: No security requirements shall be placed on the UE that requires UE to be customised to a particular customer prior to the point of sale.

C.2 Requirements on MBMS transport Service signaling protection

- R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS transport service signaling on the Gmb reference point.

NOTE: This requirement may be fulfilled by physical or proprietary security measures if the Gmb protocol endpoints (i.e. GGSN, Gmb-Proxy and BM-SC) are located within the same security domain of the operator's network. Otherwise the security mechanisms as specified within 33.210 [13] shall be applied.

~~Editor's Note: When the Gmb reference point is IP-based then NDS/IP methods according to TS 33.210 may be applied to fulfill requirement R3a. The Gmb interface is ffs.~~

- R3b: Unauthorized modification, insertion, replay or deletion of all transport service signaling, on the RAN shall be prevented when the RAN selects a point-to-multipoint (ptm) link for the distribution of MBMS data to the UE.

NOTE: UTRAN Bearer signalling integrity protection will not be provided for point to multipoint MBMS signalling and GERAN has no bearer signalling integrity protection, even for point to point signalling.

C.3 Requirements on Privacy

- R4a: The User identity should not be exposed to the content provider or linked to the content in the case the Content Provider is located outside the 3GPP operator's network.
- R4b: MBMS identity and control information shall not be exposed when the RAN selects a point-to-multipoint link for the distribution of MBMS data to the UE.
- NOTE: UTRAN and GERAN Bearer confidentiality protection will be not be provided for point to multipoint MBMS sessions.

C.4 Requirements on MBMS Key Management

- R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.
- R5b: The transfer of the MBMS keys between the MBMS key generator and the UE shall be integrity protected.
- R5c: The UE and MBMS key generator shall support the operator to perform re-keying as frequently as it believes necessary to ensure that:
- users that have joined an MBMS User Service multicast service, but then left, shall not gain further access to the MBMS User Service without being charged appropriately
 - users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User Service without having been charged appropriately
 - the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.
- R5d: Only authorized users that have joined an MBMS User Service shall be able to receive MBMS keys delivered from the MBMS key generator.
- R5e: The MBMS keys shall not allow the BM-SC to infer any information about used UE-keys at radio level (i.e. if they would be derived from it).
- R5f: All keys used for the MBMS User Service shall be uniquely identifiable. The identity may be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when an update was missed or was erroneous/incomplete.
- R5g: The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).
- R5h: The function of providing MTK to the ME shall only deliver a MTK to the ME if the input values used for obtaining the MTK were fresh (have not been replayed) and came from a trusted source.

C.5 Requirements on integrity protection of MBMS User Service data

- R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service data sent to the UE on the radio interface. The use of integrity shall be optional.
- NOTE: It may be possible to detect the deletion of MBMS data packets, but it is impossible to prevent the deletion. Packets may be lost because of bad radio conditions, providing integrity protection will not help to detect or recover from this situation.
- NOTE: The use of shared keys (integrity and confidentiality) to a group of untrusted users only prevents attacks of lower levels of sophistication, such as preventing eavesdroppers from simply listening in
- R6b: The MBMS User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.
- R6c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.

C.6 Requirements on confidentiality protection of MBMS User Service data

- R7a: It shall be possible to protect the confidentiality of MBMS User Service data on the radio interface.
- R7b: The MBMS User Service data may be encrypted with common encryption keys, which shall be available to all users that have joined the MBMS User Service.
- R7c: It may be required to encrypt the MBMS User Service data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.
- R7d: It shall be infeasible for a man-in-the-middle to bid down the confidentiality protection used on protect the MBMS User Service from the BM-SC to the UE.
- R7e: It shall be infeasible for an eavesdropper to break the confidentiality protection of the MBMS User Service when it is applied.

C.7 Requirements on content provider to BM-SC reference point

- R8a: The BM-SC shall be able to authenticate and authorize a 3rd party content provider that wishes to transmit data to the BM-SC.
- R8b: It shall be possible to integrity and confidentiality protect data sent from a 3rd party content provider to the BM-SC.
- NOTE: This reference point will not be standardised.

===== **END CHANGE** =====