**3GPP TSG-SA3 Meeting #36**
**Shenzhen, China, 23-26 October 2004**

***Tdoc ⌘S3-041009***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.246** **CR** **026** ⌘**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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Specify CSB-ID format |
| ***Source:*** | ⌘ | Siemens |
| ***Work item code:*** | ⌘ | MBMS |
| ***Date:*** | ⌘ | 22/10/2004 |
| ***Category:*** | ⌘ | **F** |
| ***Release:*** | ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | It needs to be specified how the Key Group-ID is put into the CSB-ID field of the MIKEY common Header, as the Key Group ID is 2 bytes long and the CSB-ID is 32 bits long.<br><br>Section 6.1 of MIKEY specifies:<br>* CSB ID (32 bits): identifies the CSB. It is RECOMMENDED that it is chosen at random by the Initiator. This ID MUST be unique between each Initiator-Responder pair, i.e., not globally unique. An Initiator MUST check for collisions when choosing the ID (if the Initiator already has one or more established CSB with the Responder). The Responder uses the same CSB ID in the response. |
| ***Summary of change:*** | ⌘ | It is proposed that the BM-SC chooses the most significant 16-bits randomly and the assigns the Key-Group-ID to the least significant bits of CSB-ID. |
| ***Consequences if not approved:*** | ⌘ | Interoperability problems may occur as it will be unspecified how the Key-Group-ID is put into CSB-ID |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.4.2, 3.4 (new) |

| ***Other specs affected:*** | ⌘ | Y | N | | ⌘ |
|---|---|---|---|---|---|
| | | | X | Other core specifications | |
| | | | X | Test specifications | |
| | | | X | O&M Specifications | |

| | | |
|---|---|---|
| ***Other comments:*** | ⌘ | S3-040858CR008 modifies the same section 6.4.2, but not the same text |

** FIRST CHANGE ***

## 3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

** END OF CHANGE ***

** LAST CHANGE ***

### 6.4.2 MIKEY common header

MIKEY shall be used with pre-shared keys as described in RFC 3830 [9].

MSKs shall be carried in MIKEY messages with a Data Type value of 0x07 in the MIKEY common header that signals that the message contains an MBMS MSK. This allows legacy MIKEY implementations to discard the message early in the processing stage. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

Once the MSK is in place in the UE, the UE can make use of the multicast MTK messages sent by the BM-SC. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret. A Data Type value of 0x08 is used in the MIKEY common header to signal that the message contains an MBMS MTK.

To keep track of MSKs and MTKs, a new Extension Payload (EXT) is added to MIKEY. The Extension contains the identities of MSKs and the MTKs (see clauses 6.3.2 and 6.3.3).

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE shall then respond with a MIKEY message containing the verification payload. In the case the server does not receive an ACK, normal reliability constructions can be used, e.g., start a timer when the message is sent and then resend the message if no ACK is received before the timer expires.

When creating a new CSB, ~~T~~the BM-SC shall assign a value to the CSB ID field of MIKEY common header in the following way: ~~shall carry the Key Group ID.~~

CSB-ID [0..15] is chosen randomly according to section 6.1 of RFC 3830 [9]

CSB-ID [15..31] = Key Group ID [0..15]

** END OF CHANGE ***