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

***Tdoc ⌘S3-041020***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.246** **CR** **029** ⌘ **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:*** | ⌘ | Removal of ID_i in MIKEY response messages for MSKs |
| ***Source:*** | ⌘ | Ericsson |
| ***Work item code:*** | ⌘ | MBMS |
| ***Date:*** | ⌘ | 25/10/2004 |
| ***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:*** | ⌘ | Correction of wrongly inserted field in a MIKEY message |
| ***Summary of change:*** | ⌘ | • Removed ID_i from the response message, since it is not needed and is not present in the MIKEY specification. |
| ***Consequences if not approved:*** | ⌘ | The usage of the MIKEY protocol will be violated without reason and there will be a waste of bandwidth. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.4.5.2 |

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

***Other comments:*** ⌘

### 6.4.5.2 MSK Verification message

If the BM-SC expects a response to the MSK-transport message (i.e., the V-bit in the MIKEY common header is equal to 1), the UE shall send a verification message as a response. The verification message shall be constructed according to section 3.1 of MIKEY, and shall consist of the following fields: HDR || TS ||~~ IDi_ ||~~ IDr || V, where ~~IDi is the ID of the BM-SC and~~ IDr is the ID of the UE. Note that the MAC included in the verification payload, shall be computed over ~~both the initiator's and~~ the responder's ID~~s~~ as well as the timestamp in addition to be computed over the response message as defined in RFC 3830 [9]. The key used in the MAC computation is the MUK_I.

| Common HDR | Common HDR |
|---|---|
| TS | TS |
| IDr | ~~IDi~~ |
| V | Dr |
| | V |

**Figure 6.6: The logical structure of the MIKEY Verification message**

The verification message shall not be sent as a response to MIKEY messages delivering MTK.

The verification message shall be constructed by the ME, except for the MAC field, and then be given to the MGV-F that will perform the MAC computation and will return the verification message appended with the MAC to the ME. The ME shall send the message to the BM-SC.