**3GPP TSG-SA WG3 Meeting S3#37**
**Sophia, France, 21-25 February, 2005**

***Tdoc ⌘S3-050116***

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **33.246** **CR** **055** ⌘ **rev** **1** ⌘ Current version: **6.1.0** ⌘

*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 [X] Radio Access Network ☐ Core Network [X]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Removal of Editors notes |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | MBMS |
| ***Date:*** | ⌘ | 21/2/2005 |
| ***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:*

| | |
|---|---|
| *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:*** | ⌘ | Some CRs from SA3#36 are incompletely implemented |
| ***Summary of change:*** | ⌘ | MIKEY key derivations were agreed to be used in S3-040858 (CR008rev1), but the CR did not remove the editor's note on the issue from clause 6.5.1: *Editor's Note: The choice between MIKEY key derivation algorithms and other suitable key derivations has not been made as there could be algorithms already in the UE*.<br><br>S3-041125 (CR010R3) introduced the usage of salt in MTK messages, but the CR missed to remove the related editor's note in clause 6.4. |
| ***Consequences if not approved:*** | ⌘ | Unnecessary Editors' notes in the specification |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.4, 6.5.1 |

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

| | | |
|---|---|---|
| ***Other comments:*** | ⌘ | |

## 6.4 MIKEY message creation and processing in the ME

~~Editor's note: The need for salting keys in processing of MIKEY messages is for further study.~~

### 6.4.1 General

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Clauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while clause 6.4.6 describes the initial processing by the ME on these messages. The final processing is done by the MBMS key Generation and Validation Function (MGV-F) and is described in clause 6.5.

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

To keep track of MSKs and MTKs, a new Extension Payload (EXT) [16] is added to MIKEY. The Extension Payload can contain the key types and identities of MSK and the MTK and Key Domain ID (see clauses 6.3.2 and 6.3.3).

****** Next Change ******

## 6.5 Validation and key derivation functions in MGV-F

### 6.5.1 General

It is assumed that the UE includes a secure storage (MGV-S). This MGV-S may be realized on the ME or on the UICC but for certain type of MBMS services the UICC shall be used as determined by the service provider. The MGV-F is implemented inside MGV-S.

~~Editor's Note: The choice between MIKEY key derivation algorithms and other suitable key derivations has not been made as there could be algorithms already in the UE.~~