

CHANGE REQUEST

33.246 **CR 055** rev - 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 Radio Access Network Core Network

Title:	Incompletely implemented CRs from SA3#36		
Source:	Ericsson		
Work item code:	MBMS	Date:	21/2/2005
Category:	F	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:	Some CRs from SA3#36 are incompletely implemented		
Summary of change:	CR007R3, removed text "Multicast" in clause 6.1. This change is handled by S3-050090 to the SA3#37meeting. S3-040997 was merged to S3-041127 (CR033rev1) in SA3#36, but the following agreed text from clause 6.3.2.1 was missed by the drafting group : "NOTE: When MCC MNC is used as key Domain identifier, the UE should not try to use it in another context. E.g. UE should not compare the received MCC MNC to parameters in radio level." 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: <i>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.</i> 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:			

Clauses affected:	6.3.2.1, 6.4.4, 6.5.1								
Other specs Affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"></td> <td style="padding: 2px;">N</td> </tr> </table>	Y	N		N		N	Other core specifications	
	Y	N							
		N							
	N								
		Test specifications							
		O&M Specifications							
Other comments:									

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Key Domain ID MSK ID

where

Key Domain ID = MCC || MNC and is 3 bytes long.

NOTE: When MCC || MNC is used as key Domain identifier, the UE should not try to use it in another context. E.g. UE should not compare the received MCC || MNC to parameters in radio level.

MSK ID is 4 bytes long and with byte 0 and 1 containing the Key Group part, and byte 2 and 3 containing the Key Number part. The Key Number part is used to distinguish MSKs that have the same Key Domain ID and Key Group part. Key Group part is used to group keys together in order to allow redundant MSKs to be deleted. The MSK ID is carried in the extension payload of MIKEY extension payload.

NOTE: It needs to be ensured that the Key Group parts are unique within an operator, i.e. two BM-SCs within an operator shall not use the same Key Group value.

If the UE receives an MSK and already contains two other MSKs under the same Key Domain ID and Key Group part, then the UE shall delete the older of these two MSKs.

~~Editor's Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.~~

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

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.~~

