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

Tdoc ⌘ S3-050117

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **037** ⌘ **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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correct the MSK verification message handling
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	21/02/2005
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:	⌘	The verification by the UICC that the inserted Time Stamp Field in the -to be signed-MIKEY packet shall match the previously handled MSK update procedure restricts the ME handling. It will cause an error if the ME would handle multiple MSK Update messages before generating the MSK verification messages. Furthermore the error handling in case the Time Stamp check would fail, is unspecified yet. From a security point of view, it has to be ensured that the ME cannot ask the UICC to sign arbitrary messages.
Summary of change:	⌘	Correct the description of MSK verification message handling for Time stamp handling. The two procedures 'MSK Update' and 'MSK verification' are combined into one procedure.
Consequences if not approved:	⌘	Parallel handling of MSK update message is not possible. More error situations for MSK updates/verification handling. A malicious ME may let the UICC sign (arbitrary) message when not needed.

Clauses affected:	⌘	6.4.5.2, Annex D

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications	⌘	TS 31.102
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

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

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 || IDr || V, where 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 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.

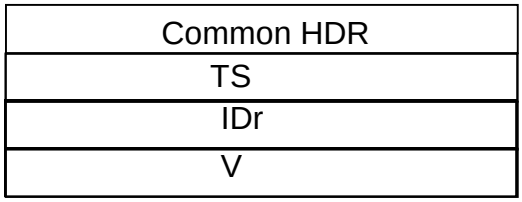


Figure 6.6: The logical structure of the MIKEY Verification message

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 verification message, when received as result from the MGV-F, ~~–~~to the BM-SC.

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

Annex D (normative): UICC-ME interface

D.1 MSK Update Procedure

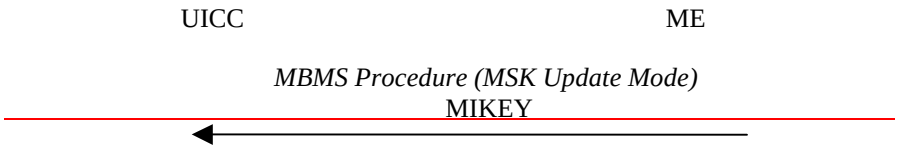
This procedure is part of the MSK update procedure as described in clause 6.5 (Validation and key derivation functions in MGV-F).

The ME has previously performed a GBA_U bootstrapping procedure as described in TS 33.220. The UICC stores the corresponding Ks_int_NAF together with the NAF_Id associated with this particular bootstrapping procedure.

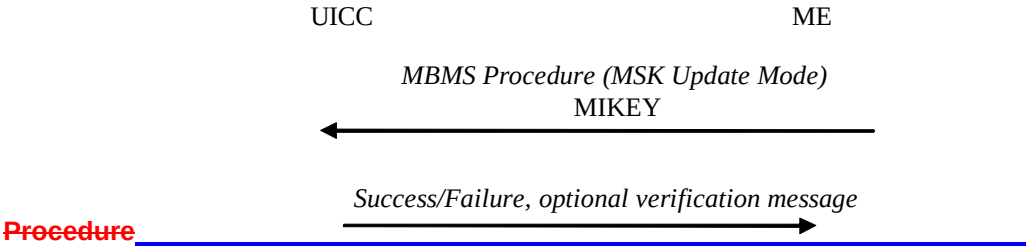
The ME receives a MIKEY message containing an MSK update ~~procedure~~. After performing some validity checks, the ME sends the whole message to the UICC. The UICC uses the MUK ID (included in the MIKEY message, see clause 6.1) to identify the stored Ks_int_NAF.

The UICC then uses Ks_int_NAF as the MUK value for MUK derivation and MSK validation and derivation (as described in clause 6.5.3).

After successful MSK Update procedure the UICC stores the Key Domain ID, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).



~~Figure D.1: MSK Update~~



~~Procedure~~

Figure D.1: MSK Update Procedure

In case the MSK update MIKEY message is acceptable (i.e. the received MSK ID corresponds to the last generated MUK in the UE, and the MSK Update procedure has been performed successfully) and the V-bit was set in the HDR, then a MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message) shall be produced. The UICC uses the same MUK ID and TS, which were received from the MSK MIKEY Message (see clause 6.1), for the MSK Verification Message Generation.

D.2 Void

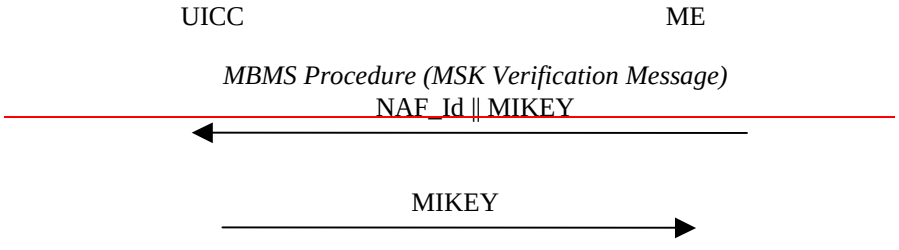
~~MSK Verification Message Generation~~

~~This procedure is part of the MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message).~~

~~The ME constructs the verification message in response to the MSK transport message when it is required by BM-SC.~~

~~The ME shall then give the constructed MIKEY verification message, with an empty MAC field, to the UICC and the ME shall include NAF_id in this message. The UICC uses the MUK ID (see clause 6.1) to identify the stored Ks_int_NAF=MUK to be used in the MSK Verification Message Generation.~~

~~The UICC will verify that the Time Stamp MIKEY field correspond to the previous MSK Update procedure. Then, the UICC shall compute and send the MIKEY packet to the ME (including the calculated MAC field) as defined in clause 6.4.5.2. (MSK Verification message).~~



~~Figure D.2: MSK Verification Message~~

D.3 MTK generation and validation

This procedure is part of the MTK generation and validation function as described in clause 6.5.4 (MTK validation and derivation).

The ME receives the MIKEY message (containing Header, Time stamp, Key Domain ID, MSK ID, MTK ID = SEQp, MSK_C[MTK||Salt (if salt is available)] and MAC). After performing some validity checks, the ME sends the whole message to the UICC. The UICC computes the MGV-F function as described in clause 6.5. (Validation and key derivation functions in MGV-F). After successful MGV-F procedure the UICC returns the MTK.

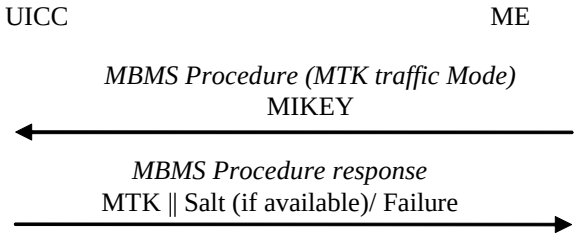


Figure D.3: MTK Generation and Validation

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