3GPP TSG SA WG3 Security – S3#34
Acapulco, Mexico, 6 –9 July 2004

S3-0400676

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **1.2.1** ⌘

*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:	⌘	UICC-ME interface for MBMS
Source:	⌘	Axalto, Gemplus
Work item code:	⌘	MBMS
Date:	⌘	07/07/04
Category:	⌘	**B**
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:	⌘	The current version of TS 33.246 does not include a description of the message needed in the UICC-ME interface.
Summary of change:	⌘	The description of the UICC-ME interface is added as normative annex.
Consequences if not approved:	⌘	Description of the solution is not complete.

Clauses affected:	⌘	Annex

Other specs affected:	⌘	Y	N		⌘
		[ ]	[ ]	Other core specifications	
		[ ]	[ ]	Test specifications	
		[ ]	[ ]	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Annex D (normative): UICC-ME interface

D.1 MSK Update Procedure

This procedure is part of the MSK update procedure as described in 6.4 (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 ME also includes in this request NAF_Id 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 chapter 6.4.1 and 6.4.2)

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

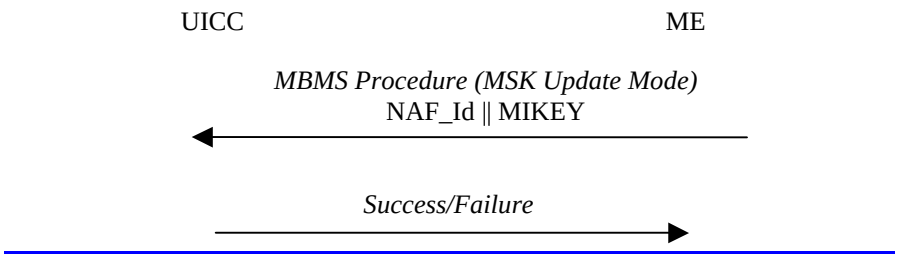

Figure x: MSK Update Procedure

D.2 MSK Verification Message Generation

This procedure is part of the MSK Verification Message as described in 6.3.6.2 (MSK Verification message)

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

The ME shall then give the constructed MIKEY verification message, with an empty MAC field, to the UICC. The ME also includes in this request NAF_Id 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 6.3.6.2. (MSK Verification message).

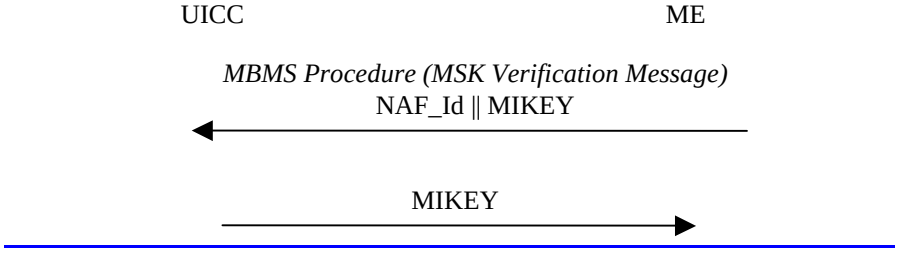

Figure x: MSK Verification Message

D.3. MTK generation and validation

This procedure is part of the MTK generation and validation function as described in 6.4.3 (MTK validation and derivation)

The ME receives the MIKEY message (containing Header, Time stamp, Network ID, Key Group ID, MSK ID, MTK ID = SEQp, MSK_C[MTK] 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 section 6.4. (Validation and key derivation functions in MGV-F). After successful MGV-F procedure the UICC returns the MTK.

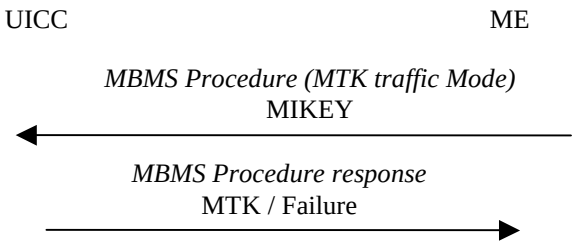

Figure x: MTK Generation and Validation