3GPP TSG-SA3 Meeting #35
Malta, 5 – 8 October

Tdoc ⌘S3-040793

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **008** ⌘ **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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	MBMS Key processing
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	20/09/2004
Category:	⌘	**C**
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:	⌘	Processing of MTKs and MSKs needed clearification
Summary of change:	⌘	• Removed heading 6.4.1, since the text in the section is more general than the heading suggests. • Removed ID_i from the response message, since it is not needed and is not present in the MIKEY specification. • Changed Sections 6.5.3 and 6.5.4, so that they now refer to the MIKEY specification instead of re-stating the same functionality again. Having the functionallity specified in two places only creates confusion. Especially, the change implies that MIKEY's built in PRF is used for key derivation. This should be prefered, since introducing a new PRF requires time consuming analysis to determine that the new PRF is secure in the new setting.
Consequences if not approved:	⌘	The usage of MTK and MSK will be underspecified.

Clauses affected:	⌘	3.2, 6.4.1, 6.4.5.2, 6.5.3, 6.5.4

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

Other comments:	⌘	

__FIRST_CHANGE__

~~3.2 Symbols~~

~~For the purposes of the present document, the following symbols apply:~~

~~MUK_I Integrity key derived from key MUK~~
~~MUK_C Confidentiality key derived from key MUK~~
~~MSK_I Integrity key derived from key MSK~~
~~MSK_C Confidentiality key derived from key MSK~~

__SECOND_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. Subclauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while subclause 6.4.6 describe 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 subclause 6.5.

~~6.4.2 MIKEY common header~~

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

MSKs shall be carried in MIKEY messages with a Data Type value of 0x07 in the MIKEY common header that signals that the message contains an MBMS MSK. This allows legacy MIKEY implementations to discard the message early in the processing stage. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

Once the MSK is in place in the UE, the UE can make use of the multicast MTK messages sent by the BM-SC. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret. A Data Type value of 0x08 is used in the MIKEY common header to signal that the message contains an MBMS MTK.

To keep track of MSKs and MTKs, a new Extension Payload (EXT) is added to MIKEY. The Extension contains the identities of MSKs and the MTKs (see subclause 6.3.2 and 6.3.3).

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE shall then respond with a MIKEY message containing the verification payload. In the case the server does not receive an ACK, normal reliability constructions can be used, e.g., start a timer when the message is sent and then resend the message if no ACK is received before the timer expires.

The CSB ID field of MIKEY common header shall carry the Key Group ID.

__THIRD_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 ~~|| 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 IDs as well as the timestamp in addition to be computed over the response message as defined in [9]. The key used in the MAC computation is the MUK_I.~~

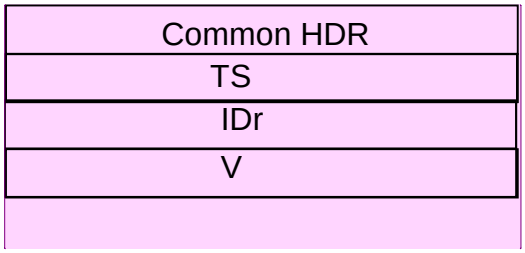

Figure 6.6: The logical structure of the MIKEY Verification message

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 message to the BM-SC.

__FOURTH_CHANGE__

6.5.2 MUK derivation

When a MUK has been installed in the MGV-S, i.e. as a result of a GBA run, it is used as pre-shared secret ~~together with the MIKEY_RAND and the Key Group ID from the MIKEY message to derive encryption and integrity keys (MUK_C and MUK_I) as defined in section 4.1.4 of MIKEY. MUK_I and MUK_C are~~ used to verify the integrity of the MSK transport message and decrypt the key carried in the KEMAC payload as described in [9].

6.5.3 MSK processing~~validation and derivation~~

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key in the message is an MSK, MGV-F retrieves the MUK with the ID given by the Extension payload.

~~The MAC in the KEMAC payload is verified using MUK_I, and the message is discarded if verification fails. If the MAC verification is successful the MUK_C is used to decrypt the Key Data sub-payload, and the MSK can be installed in the MGV-S. The MSK is used as pre-shared secret together with the MIKEY_RAND and the Key Group ID from the MIKEY message to derive (as specified in section 4.1.4 of [9]) encryption and integrity keys (MSK_I and MSK_C).~~ The integrity of the message is validated and the MSK is extracted from the KEMAC payload as described in Section 5 of [9] if the validation is successful. The Key Validity data is extracted from the message and stored (in the form of MTK ID interval). The lower limit of the interval defines the SEQs.

NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. to update the Key Validity data.

If message~~MAC verific~~validation is successful, then the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MUK ID.

6.5.4 MTK processing~~validation and derivation~~

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall verify the integrity of the MIKEY message according to [9]. ~~calculate the MAC as defined in [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message~~. If the ~~MAC~~ verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the ~~MAC~~ verification is successful, then the MGV-F shall update SEQs with SEQp value and extract the ~~start the generation of~~ MTK from the message. The MGV-F then provides the MTK to the ME.

The MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of MIKEY [9].