3GPP TSG-SA3 Meeting #36
Shenzhen, China, 23 – 26 November 2004

Tdoc ⌘S3-041118

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**	**010**	⌘**rev**	**2**	⌘	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⌘ ☒ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	MBMS Transport of salt		
Source:	⌘	MBMS drafting group		
Work item code:	⌘	MBMS	***Date:*** ⌘	23/11/2004
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:	⌘	The protection of the MBMS traffic will not meet the commonly required design goal of having a security level equivalent to the key size.
Summary of change:	⌘	The salt needed by SRTP is sent in the KEMAC payload of the MIKEY message containing the MTK.
Consequences if not approved:	⌘	The protection of the MBMS traffic will be vulnerable to pre-computation attacks.

Clauses affected:	⌘	6.4.5.3, 6.4.6.2, 6.5.4, D.3				
		Y	**N**			
Other specs Affected:	⌘	X		Other core specifications	⌘	TS 31.102
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

__FIRST_CHANGE__

6.4.5.3 MTK message structure

The structure of the MIKEY message carrying a MTK key is depicted in Figure 6.7. The actual key that is delivered is kept in the KEMAC payload. If MTK is to be used for streaming protection, then a 128 bit salt shall be added to the KEMAC payload in addition to the MTK. The network identity payloads (IDi) shall be used in MTK transport messages.

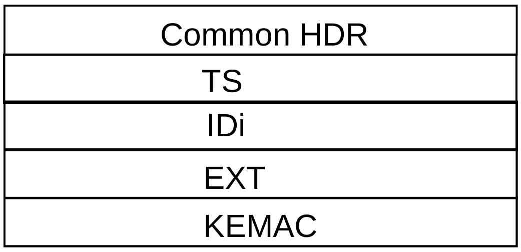

Figure 6.7: The logical structure of the MIKEY message used to deliver MTK

__SECOND_CHANGE__

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MTSK delivery, the MSK ID is extracted from the Extension Payload.
2. The Timestamp Payload is checked, and the message is discarded if the counter is larger or equal to the current MIKEY replay counter associated with the given MSK (the counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than´´ should be in the sense of RFC1982 [10].
3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message shall be discarded.
4. The message is transported to MGV-F for further processing, cf 6.5.3.
5. The MGV-F replies success (i.e. sending the MTK and salt when available) or failure.

__THIRD_CHANGE__

6.5.4 MTK 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 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 start the generation of MTK. The MGV-F 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.

In the case of streaming, SRTP requires a master key and a master salt. The MTK is used as master key, and the salt in the KEMAC payload is used as master salt.

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].

__FOURTH_CHANGE__

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, Network ID, Key Group ID, MSK ID, MTK ID = SEQp, MSK_C[MTK||Salt (when 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.

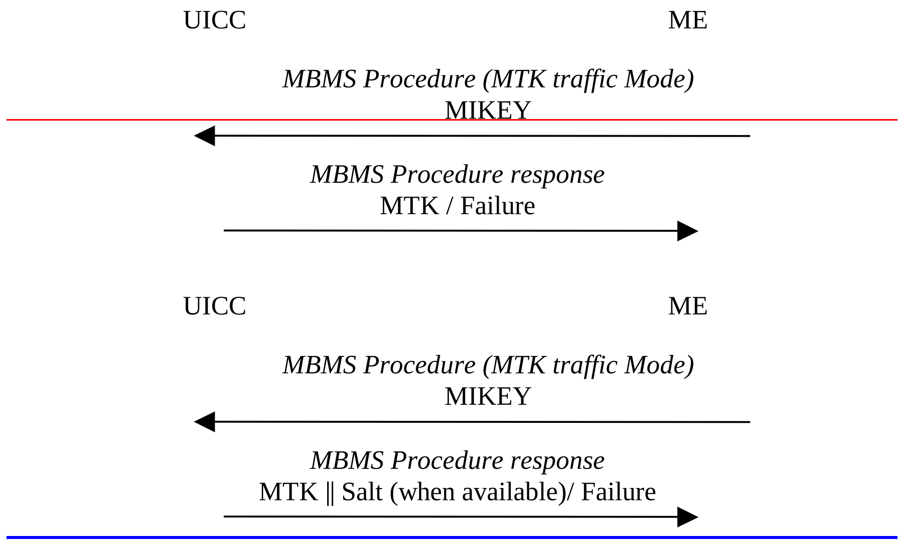
UICC
ME
MBMS Procedure (MTK traffic Mode)
MIKEY
MBMS Procedure response
MTK / Failure
UICC
ME
MBMS Procedure (MTK traffic Mode)
MIKEY
MBMS Procedure response
MTK || Salt (when available)/ Failure

Figure D.3: MTK Generation and Validation