3GPP TSG SA WG3 Security — S3#37 **S3-050088**
21-25 February 2005
Sophia Antipolis, France

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **049** ⌘ **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: ⌘ MGV-F functionality related to MTK-ID upper limit

Source: ⌘ Samsung Electronics

Work item code: ⌘ MBMS ***Date:*** ⌘ 13/02/2005

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:

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: ⌘ There is no statement of the MGV-F functionality which is related to the MTK-ID upper limit.

Summary of change: ⌘ Add the MGV-F functionality which is related to MTK-ID upper limit.

Consequences if not approved: ⌘ Arbitrary implementation of the MTK-ID upper limit related MGV-F functionality may lead to MGV-F wrong operation.

Clauses affected: ⌘ 6.4.5.1, 6.5.3, 6.5.4

Other specs Affected: ⌘

Y	N		
	N	Other core specifications	⌘
	N	Test specifications	
	N	O&M Specifications	

Other comments: ⌘

********** START OF CHANGE **********

6.4.5.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depicted in Figure 6.5. The actual key that is delivered is kept in the KEMAC payload. The MIKEY-RAND is used to derive e.g. encryption and authentication keys from the received keys. It is sent in all the MSK delivery messages. The identity payloads of the initiator's and responder's IDs shall be included in the MSK transport messages. IDi is the ID of the BM-SC (i.e. NAF-ID) and IDr is the ID of the UE's username (i.e.B-TID). Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. The Key Validity Data subfield is present in the KEMAC payload when MSK is transported but it is not present for MTK transport. The field defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). The lower limit of the interval defines the SEQs to be used by the MGV-F (see clause 6.5). The upper limit of the interval defines the SEQu.

********** NEXT CHANGE **********

6.5.3 MSK validation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the EXT. If the key in the message is an MSK protected by MUK, MGV-F retrieves the MUK identified as specified in clause 6.1.

The integrity of the message is validated and the MSK is extracted from the KEMAC payload as described in section 5 of reference [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. The upper limit of the interval defines the SEQu.

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 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.

********** NEXT 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 EXT. If the key inside the message is an MTK protected by MSK, 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 numbers SEQs and SEQu, have been stored within a secure storage (MGV-S). ~~Both~~ MSK~~ and~~, SEQs and SEQu were transferred to the MGV-S with the execution of the MSK update procedures. The initial values of SEQs and SEQu ~~is~~ are 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 and SEQu. If SEQp is equal or lower than SEQs, or SEQp is greater than SEQu, then the MGV-F shall indicate a failure to the ME. ~~If SEQp is greater than SEQs then~~Otherwise, the MGV-F shall verify the integrity of the MIKEY message according to RFC 3830 [9]. If the verification is unsuccessful, then the MGV-F will indicate a failure to the

ME. If the verification is successful, then the MGV-F shall update SEQs with SEQp value and extract the MTK from the message. The MGV-F then provides the MTK to the ME.

If MAC verification is successful, 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 RFC 3830 [9] (MIKEY).

In case of download service, MIKEY key derivation as defined in section 4.1.3 of MIKEY [9] shall be used to derive MTK authentication and encryption keys from MTK in the ME. These keys shall be provided to the download protection protocol.

********** END OF CHANGE **********