3GPP TSG-SA3 Meeting #35
St Pual's Bay, Malta, October 5 – 8, 2004

Tdoc ⌘S3-040814

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**	**018**	⌘ **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⌘ ☒ ME ☒ Radio Access Network □ Core Network ☒

Title:	⌘	Clarification of the format of MTK ID and MSK ID.		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	28/09/2004
Category:	⌘	**C**	***Release:*** ⌘	Rel-6

Use one of the following categories:	*Use one of the following releases:*
F *(correction)*	*2 (GSM Phase 2)*
A *(corresponds to a correction in an earlier release)*	*R96 (Release 1996)*
B *(addition of feature),*	*R97 (Release 1997)*
C *(functional modification of feature)*	*R98 (Release 1998)*
D *(editorial modification)*	*R99 (Release 1999)*
Detailed explanations of the above categories can	*Rel-4 (Release 4)*
be found in 3GPP TR 21.900.	*Rel-5 (Release 5)*
	Rel-6 (Release 6)

Reason for change: ⌘ The format of MSK ID and MTK ID is unclear. According to the TS they are used as sequence numbers, but this needs to be clarified in the text.

From 6.4.4:
When an MSK is delivered to a UE, the MIKEY message contains an EXT that holds the MUK ID of the MUK used to protect the delivery, and the MSK ID of the MSK delivered in the message. For messages that contain an MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. **The MSK ID and MTK ID are increased by 1 every time the corresponding key is updated**. It is possible that the same MTK is delivered several times in multicast, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

Summary of change: ⌘ The format of MSK ID and MTK ID are clarified.
MSK ID is a sequence number and it shall be increased by 1 modulo 2exp<key id length>, when MSK is updated.

MTK ID is a sequence number with length of 4 bytes and it shall be increased by 1 modulo 2exp<key id length>, when MTK is updated.

Consequences if not approved: ⌘ MSK IDs and MTK IDs remains unclear.

Clauses affected: ⌘

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

Other comments: ⌘

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Network ID, Key Group ID and MSK ID

where

Network ID = MCC || MNC and is 3 bytes long. It is carried in the IDi payload in MIKEY message

Key Group ID is 2 bytes long and is used to group keys together in order to allow redundant MSKs to be deleted. It is carried in the CSB ID field of MIKEY common header.

MSK ID is 2 bytes long sequence number and is used to distinguish MSKs that have the same Network ID and Key Group ID. It is carried in the MSK-ID field of MIKEY extension payload. The MSK ID shall be increased by 1 modulo $2^{(\text{MSK ID length})}$ every time the MSK is updated.

If the UE receives an MSK and already contains two other MSKs under the same Network ID and Key Group ID, then the UE shall delete the older of these two MSKs.

Editor's Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.

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

6.3.3.1 MTK identification

Every MTK is uniquely identifiable by its Network ID, Key Group ID, MSK ID and MTK ID

where

Network ID, Key Group ID and MSK ID are as defined in subclause 6.3.2.1.

MTK ID is 4 bytes long sequence number and is used to distinguish MTKs that have the same Network ID, Key Group ID and MSK ID. It is carried in the MTK-ID field of MIKEY extension payload. The MTK ID shall be increased by 1 modulo $2^{(\text{MTK ID length})}$ every time the MTK is updated. The MTK ID shall be reset every time the MSK is updated.

~~Editor's Note: The format of MTK is ffs.~~

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

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in MIKEY [9]. To be able to keep track of the keys, a new general Extension Payload (EXT) is defined that conforms to the structure defined in 6.15 of MIKEY[9]. The IDs of the involved keys are kept in the EXT, to enable the UE to look up the identity of the key which was used to protect the message, and which key is delivered in the message. This EXT is incorporated in the MIKEY messages (see Figure 6.4). When an MSK is delivered to a UE, the MIKEY message contains an EXT that holds the MUK ID of the MUK used to protect the delivery, and the MSK ID of the MSK delivered in the message. For messages that contain an MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. Cf. subclauses 6.3.2.1 and 6.3.3.1 for definition of MSK ID and MTK ID. The MSK ID and MTK ID are increased by 1 modulo $2^{(\text{key ID length})}$ every time the corresponding key is updated. It is possible that the same MTK is delivered several times in multicast, and the ME can then discard messages related to a key it already has instead of passing them to the MGV-F.

The MGV-F (see subclause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integer counters, different from zero. The reason for disallowing zero is that it is reserved for future use. Note that this means that there can only be 2^{n} - 1 different keys in use during the same session, where n is the number of bits in the ID field.

Outer Key ID	Inner Key ID

Figure 6.4: Extension payload used with MIKEY

The Inner Key ID is the ID of the key that is transported in the message (i.e. an MSK or MTK). The Outer Key ID is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK).