3GPP TSG SA WG3 Security — SA3#35 **S3-040754**

October 5-8, 2004, St Paul's Bay, Malta

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **003** ⌘ **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:	⌘	**Delivery of multiple keys in one MIKEY message for MBMS**
Source:	⌘	Samsung Electronics
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:	⌘	MIKEY itself can support of the delivery of one or more keys(i.e.TGKs) from the initiator to the responder. But currently special for MBMS, one MIKEY message can be used to transmit only one key (MSK or MTK). Since an MBMS user service may use one or more MSKs (and MTKs accordingly) at the same time, multiple MIKEY messages have to be used for delivery of these multiple MSKs (MTKs).
Summary of change:	⌘	Change the EXT payload to support the delivery of multiple keys.
Consequences if not approved:	⌘	Multiple MIKEY messages have to be used to deliver multiple keys, which is a waste of resources.

Clauses affected:	⌘	6.4.4

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

⌘

Other comments: ⌘

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

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the keys, a new general Extension Payload (EXT) with variable length is defined that conforms to the structure defined in section 6.15 of RFC 3830 [9] (MIKEY). 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~~ MSKs ~~is~~ are 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 IDs of the MSKs delivered in the message. For messages that contain ~~an~~ MTKs, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK IDs of the MTKs 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.

The MGV-F (see clause 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.

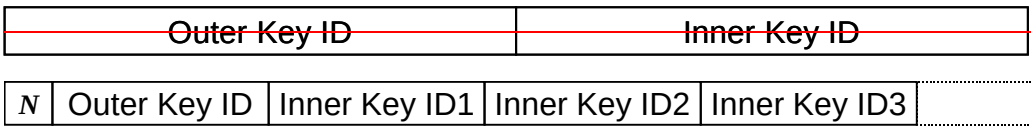

Figure 6.4: Extension payload used with MIKEY

Integer ***N*** indicates how many actual MSKs or MTKs that are delivered are kept in the KEMAC payload of the MIKEY message, and also the number of Inner key IDs. 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).