3GPP TSG SA WG3 Meeting S3#35
St Paul's Bay, Malta, 5 ñ 8 October 2004

Tdoc ⌘S3-040833

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**022**	⌘**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 ☐

Title:	⌘	Modification of delivery of MIKEY RAND field in MSK updates		
Source:	⌘	Axalto, Gemplus		
Work item code:	⌘	WLAN	***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:

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: ⌘ Currently, TS states that MIKEY-RAND is only delivered in the first MIKEY packet containing an MSK update message. Basically, that imposes to the MGV-F the need to store MIKEY-RAND together with a given MUK for further MUK & MSK derivation. That also implies that when receiving MSKs from different BMSCs (e.g. roaming situations) the storage of multiple MUK and associated MIKEY_RAND parameter (one per BMSC) is required.

Contrary to MUK, which can be derived in the UE from existing GBA keys, there is no way to retrieve MIKEY_RAND value if for any reasons it is missed or replaced.

If that happens, the BM-SC cannot be aware that MIKEY RAND is no more present in the UE. So, if the same MUK is used again to deliver a MSK, BM-SC will not include MIKEY-RAND in his MSK update message. As a consequence MUK & MSK derivation procedures cannot take place and the MSK update procedure will fail.

Summary of change: ⌘ MIKEY RAND is sent in all MSK update MIKEY packets. MIKEY RAND will be used for MUK derivation whenever MUK_C and MUK_I are not present. MIKEY RAND will always be used for MSK derivation (MSK_I and MSK_C) whenever a new MSK is sent.

Then, the MGV-F does not need to store MIKEY_RAND fields.

Consequences if not approved: ⌘ Unnecessary complexity in handling replacement of MUK and associated parameters.

Possible scenarios where MSK update procedure are not possible unless a complete GBA bootstrap procedure is performed.

Clauses affected: ⌘

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

Other comments: ⌘

6.4.5 MIKEY message structure

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 ~~only~~ in all the ~~initial~~ MSK delivery messages. The identity payloads of the initiatorís and responderís IDs shall be included in the MSK transport messages. IDi is the ID of the BM-SC and IDr is the ID of the UE. 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 subclause 6.5).

Editorís Note: The type (URI or NAI) of identity payloads to use are for further study.

Editorís Note: The contents of the Security Policy payload depends on the used security protocols. MIKEY [9] has defined Security Policy payload for SRTP, but for other security protocols there is a need to define new Security Policy payloads. The exact definitions of these are FFS.