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

Tdoc ⌘S3-040744

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **002** ⌘ **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 [X]

Title:	⌘	Ericsson comments to Clarification on key management
Source:	⌘	Orange
Work item code:	⌘	MBMS
Date:	⌘	24/09/2004
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:	⌘	Alignment with TS 22.146. CR to TS 22.146 SP 040696 which was approved at SA#25 states : " If a terminal supports MBMS, then it shall support UICC based key management and all the function and interfaces required for it. In addition, ME key management shall be supported. If the UICC is capable of MBMS key management, ME key management shall not be activated." The consequence of the last sentence may be an interoperability problem if the network does not support UICC key management. Then the UE will not get access to a ME based service even though UE supports both ME and UICC key managements. It is proposed that SA3 reconsiders the requirement: *If the UICC is capable of MBMS key management, ME key management shall not be activated.*
Summary of change:	⌘	Clarify that UICC based key management is used when UICC is capable of MBMS key management and that ME based key management is used when UICC is not capable of MBMS key management.
Consequences if not approved:	⌘	Misalignment between TS 22.146 and TS 33.246

Clauses affected:	⌘	3.1, 6.1

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

***** Begin of change *****

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply.

For the definitions of MBMS User Service refer to [5].

MRK = MBMS Request Key: This key is to authenticate the UE to the BM-SC when performing key requests etc.

MSK = MBMS Service Key: The MBMS Service key that is securely transferred (using the key MUK) from the BM-SC towards the UE. The MSK is not used directly to protect the MBMS User Service data (see MTK).

MTK = MBMS Traffic Key: A key that is obtained by the UICC or ME by calling a decryption function MGV-F with the MSK. The key MTK is used to decrypt the received MBMS data on the ME.

MUK = MBMS User Key: The MBMS user individual key that is used by the BM-SC to protect the point to point transfer of MSK's to the UE.

NOTE: The keys MSK and MUK may be stored within the UICC or the ME depending on the ~~MBMS service~~UICC capabilities.

***** End of change *****

***** Begin of change *****

6 Security mechanisms

6.1 Using GBA for MBMS

GBA[6] is used to agree keys that are needed to run an MBMS Multicast User service. MBMS imposes the following requirements on the MBMS capable UICCs and MEs:

A UICC that contains MBMS key management functions shall implement GBA_U.

An ME that supports MBMS shall implement GBA_U and GBA_ME, and shall be capable of utilising the MBMS key management functions on the UICC.

Before a user can access an MBMS User service, the UE needs to share GBA-keys with the BM-SC. If no valid GBA-keys are available at the UE, the UE shall perform a GBA run with the BSF of the home network as described within [6] clause 5. The BM-SC will act as a NAF according to [6].

The MSKs for an MBMS User service shall be stored on either the UICC if the UICC is capable of MBMS key management or the ME if the UICC is not capable of MBMS key management.

~~-~~Storing the MSKs on the UICC requires a UICC that contains the MBMS management functions (and that is GBA aware) and requires that the BM-SC is GBA_U aware. As a result of the GBA_U run in these circumstances, the BM-SC will share a key Ks_ext_NAF with the ME and share a key Ks_int_NAF with the UICC. This key Ks_int_NAF is used by the BM-SC and the UICC as the key MUK to protect MSK deliveries to the UICC as described within subclause 6.3. The key Ks_ext_NAF is used as the key MRK within the protocols as described within subclause 6.2.

NOTE: A run of GBA_U on a GBA aware UICC will not allow the MSKs to be stored on the UICC, if the MBMS management functions are not present on the UICC.

In any other circumstance, a run of GBA results in the BM-SC sharing a key Ks_(ext)_NAF with the ME. This key Ks_(ext)_NAF is used by the BM-SC and the ME to derive the key MUK and the key MRK (MBMS Request Key). The key MUK is used to protect MSK deliveries to the ME as described within subclause 6.3. The key MRK is used to authenticate the UE towards the BM-SC within the protocols as described within subclause 6.2.

Ericsson: Consider the following cases. It is assumed that the network may choose between UK and MK per service.

UK : UICC based key management

MK: ME based key management

Case	UICC	ME	Network	Resulting key management
1	UK	UK/MK	UK/MK	UK / MK (operator choice but UK should be preferred)
2	-	UK/MK	UK/MK	MK
3	UK	UK/MK	MK	MK or no service?
4	-	UK/MK	MK	MK
5	UK	UK/MK	UK	UK
6	-	UK/MK	UK	No service possible

As can be seen, in case 3 both the ME and network would be capable of ME based key management, but due to the new requirement service is not possible. To overcome this problem, the decision between UICC or ME based key management should be based on network decision and not on UICC capabilities.

Consider the following example. A user has configuration in case 4. He is able to receive ME based services. When he updates the UICC and moves to configuration in case 3 he is not anymore able to receive the ME based services.

***** End of change *****