3GPP TSG SA WG3 Security — SA3#33 **S3-040220**
10-14 May 2004
Beijing, China

Source:	**Siemens**
Title:	**MBMS: Use of Registration Keys.**
Document for:	**Discussion and decision**
Agenda Item:	**MBMS**

1 Introduction

This contribution analyses and compares the key layers that are needed within the different key management models that were known at SA3#32. The conclusion of this paper is that the use a 'Registration Key' intended tight to subscription as proposed by the OTA-model is misleading; it needs further specification and adds additional complexity to MBMS keys management.

2 Definition and purpose a Registration Key

As the idea of a separate Registration Key (RK) for MBMS has been introduced through the 3GPP2-model [BCMCS], we first recapitulate the purpose of it as was introduced within [BCMCS]:

> *"RK Registration Key, A Key on the UICC which is User individual (different from the UMTS key K) and is used to obtain the BAK through generating an intermediate Key on the UICC and the Network that is used to encrypt the BAK transfer. How to put the RK on the UICC has not been standardized.*
>
> *BAK Broadcast Access Key, the key on the UICC which is service specific and used for the generation of Session Keys.*
>
> *SK Session Key: The actual key that protects the MBMS traffic. "*

From the above description it is clear that the RK is an MBMS User Service related key which the user receives from subscription[1]. In the 3GPP2 network model the registration key is actually owned by a subscription manager outside of the operator's network whereby the network operator multicasts the content towards the mobile users.

The business model for 3GPP MBMS is different from the 3GPP2 model, as in the 3GPP model the MBMS user services are always owned by the mobile network operator. The network operator is always the one the user subscribes to. The secure relationship between the user and the subscription owner therefore already exists, as is available in the form of the key K on the UICC. In effect, this particular optimization case has been acknowledged by 3GPP2 as has been stated within [BCMCS] Section 4.3.1 as quoted in following *italic* text:

> *"Subscription Manager (SM): May provide the functions of Authentication, Authorization and Accounting (AAA).*
>
> *The SM shares a Registration Key RK with the UIM: This key RK may be the A-key (which is the basis of key distribution and authentication for voice/data services as described in S.S0053), the key K used for AKA (as described in S.S0055), or some other key provisioned specifically for BCMCS. The SM calculates the TK, based on the user specific RK. The provisioning of RK in the UIM and SM is beyond the scope of this"*

The use of GBA [TS33.220] (in both variants GBA_U and GBA_ME) is based on deriving a key MUK from the Key K, and then using this key MUK to transfer MSK to the UE. This provides a similar solution as with a 'temporary' key TK derived from the Key K. The provision of the key RK and the standardization of the interfaces to use for it can therefore be omitted in a GBA based solution.

[1] The fact that it has not been standardized how the RK is transferred towards the UE could lead to interoperability problems between the RK-owner and the UE, but this is only a side issue in the discussion on the necessity of the registration key.

Following table compares roughly the use of keys as proposed in [S3-040088], [BCMCS], GBA-based and TS33.246 v110.

Key Name and function	TS 33.246	S3-040088 (OTA-based)	BCMCS	GBA-based	Comments
UICC Card Key K (user access authentication)	x	x	x	x	No difference
OTA secure packet delivery Key		x – NOTE 1	?? Standardization left open	No	
Registration Key (RK)		x – NOTE 2 and 3	Yes if SM outside of mobile network	No	
MBMS User specific key (MUK)	x	????	TK (temporary Key)	Yes, established via GBA	
MBMS Service Key (MSK)	x	BAK	BAK	x	No difference
MBMS Traffic Key (MTK)	x	x	SK	x	No difference

NOTE 1: These keys would be semi-static and managed by OTA, and therefore independent from MBMS. The OTA key could be considered as a User Specific Key.

NOTE 2: [S3-040088] describes in section 6.2.1 of the proposed pCR: '*MBMS Registration keys (RK) are used to protect BAK delivery to the UICC. RK may be different for each subscriber.*' This indicates that the purpose of the Registration Key as used in [S3-04088] is not the same as for [BCMCS]. We derive that fact also from the absence of any text within [S3-040088] that indicates that a temporary key TK is derived from RK before effectively encrypting the key BAK (i.e. MSK).

NOTE-3: [S3-040088] indicates "*RK may be different in VN and HN case*". This text sounds strange in the sense that for [BCMCS] that key is assigned by the subscription manager which indicates it to have a service specific property (and not specific to a network). In the case of [S3-040088] the key RK seems not to have the property of a key RK of [BCMCS].

In addition to the above cited RK-phrases in [S3-040088] that cause confusion on its actual properties, one need also to mention why there is a need for the additional RK-based key layer. As the OTA-based solution is necessarily a Home-network based solution[2], the BM-SC needs to protect the MSK transfer with an additional key[3].

[2] As there exist different OTA card variants

[3] in addition to the OTA encryption and access control.

3 Conclusion

This paper has compared the different keys usages in the OTA and GBA-based model. The conclusions are:

1) The purpose and use of the key RK in [S3-040088] is unclear. [S3-040088] even more hints that its purpose is different from the Registration Key as known from [BCMCS] for the purpose of subscription. Therefore the name *registration key* is misleading in [S3-040088].

2) An additional key layer as in [S3-040088] based on RK can be avoided as shown in [BCMCS] and GBA-based models. However the use of OTA (as being a HN based system) seems to necessity its use.

3) It is yet unspecified how the key RK in [S3-040088] will be actually used together with an encryption algorithm.

It is proposed to adopt the working assumption that preference shall be given to those key management proposals that only implement MUK-MSK-MTK. The management of additional keys above the mentioned key hierarchy of TS33.246 is seen as an unnecessary complication of the key management solution.

4 References

[BCMCS]: S.R0083-0_v1.0_111103: 3GPP2 Broadcast-Multicast Service Security Framework; http://www.3GPP2.org

[S3-040051]: Discussion paper on MBMS key management, SA2#32, Axalto et al

[S3-040088]: CR on MBMS key Management procedures, AXALTO, Gemplus, Oberthur, SA3#32

[TS33.220]: SP-0400164: TS 33.220v600: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture" for Release 6.