3GPP TSG SA WG3 Security — SA3#33 **S3-040449**
10-14 May 2004
Beijing, China

Source:	**MBMS Security Rapporteur**
Title:	**Update of Editor's note in TS to reflect decisions made in SA3#33**
Document for:	**Discussion and decision**
Agenda Item:	**MBMS**

1 Introduction

The attached pseudo-CR proposes changes to editor's notes in the MBMS TS to reflect decisions at SA3#33.

First Change

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.

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

Editors Note: How the MSK is used for download is still under study.

MTK = MBMS Traffic Key: A key that is obtained by the ME by calling a function fx (MSK, Key-deriv parameters). The key MTK is used to decrypt the received MBMS data on the ME.

~~Editors Note on MSK and MTK: These definitions are subject to further modification as two alternative two-tiered keying systems are still under consideration a) the SK_RAND model b) the key encryption model. For Case a) fx may be a PRF (hash function) while for case b) an encryption algorithm is needed. Key-deriv will be RAND for case a). For case b) Key-deriv will be a MTK encrypted with key derived from MSK.~~

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.

Editors Note: The keys MSK and MUK may be stored within the UICC or the ME depending on the MBMS service. The function fx may be realized on the ME or the UICC

End of first change

Second Change

5 MBMS security functions

5.1 Authenticating and authorizing the user

A UE is authenticated and authorised in two parts when participating in an MBMS service. Firstly when the UE establishes a bearer to receive MBMS traffic and secondly when the UE request and receive keys for the MBMS service. The bearer establishment authentication is performed using the normal network security described in TS 33.102 [4]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish a bearer (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the network (i.e. controlled by the BM-SC), there is an additional procedure to remove a MBMS bearer related to a UE that is no longer authorised to access the MBMS service.

Editor's Note: It was agreed that the GBA method will be used for MBMS Security (GBA-U + GBA-ME + MIKEY). It was agreed that the work would continue under the assumption of there being both the UICC-based solution and ME-based solution. If a Terminal is to support MBMS, then it will need to support GBA-U.

~~Editor's note: It was agreed to standardise a solution that allowed MBMS specific keys to be stored in either the ME or UICC in release 6. The choice of storage depends on whether the UICC has the ability to hold the keys or not. The differences between the two methods will only be visible in the UE, and the BM-SC would know which method of storing the keys in the UE will be used.~~

~~Editor's note: The use of AKA between the BM-SC and UE was proposed. It was concluded that the issue of bootstrapping and having the BM-SC in the visited network need to be further investigated.~~

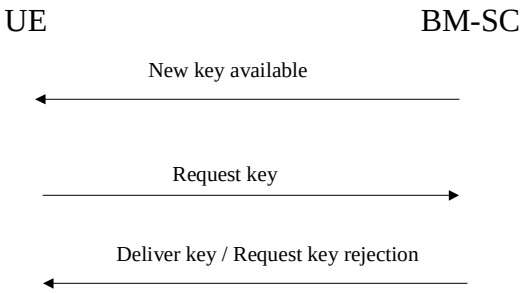
End of second change

Third Change

6.2 Key update procedure

Once a UE has joined a multicast service, the UE should try to get the MSK that will be used to 'protect' the data transmitted as part of this multicast service. If the UE fails to get hold of the MSK or receives confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still-valid, older MSK, the UE shall leave the MBMS user service. The UE tries to get the MSK using the second message in the below flow.

The BM-SC controls when the MSKs used in a multicast service are to be changed. The below flow describes how MSK changes are performed.



The first message is sent out by the BM-SC to indicate that new MSKs are available. It is an optional message in the flow. If it is sent to all UEs, then the BM-SC should provide the rules to the UE for subsequent request for the new MSK when a UE joins a multicast service, to avoid simultaneous requesting from all the UEs.

Editor's note: A possible method for achieving the above is for the BM-SC to allocates different "request delay time" to different UEs; such that when the UEs receive the new key available message, they shall send the request key message after the delay requested by the BM-SC. Alternatively it is possible to use the key lifetime methods suggested in S3-040059.

The second message is used to request an MSK. This is sent by the UE when it either receives the first message in the flow and does not have the new MSK, or has just joined a multicasts service and does not have an MSK for that service or has received some protected content and does not have the MSK that was used to protect the content. If the UE fails to get hold of the updated MSK or receive confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still valid older MSK, the UE shall leave the MBMS service.

After receiving the second message the BM-SC should send out the appropriate MSK to the UE protected by the relevant means, or reject the UE's key request with an indication of the cause. Upon successfully receiving the new MSK, the UE should store this key for later use.

~~Editor's note: If OTA is used to carry MSKs to the UICC, the following recommendations shall be followed:~~

~~- OTA should not use DES in CBC mode,~~

~~- The keys used for the ptp transporting of MSK to the UICC shall not be shared among subscribers,~~

- ~~OTA should not rely on the same keys for transporting MBMS data and other application data towards the UICC.~~

Editor's note: MIKEY was ~~is being considered~~chosen as the method for carrying keys. The use of MIKEY will be based on the proposal in S3-040258. ~~Possible optimisations were proposed at the ad-hoc in Antwerp (S3z030010). One identified issue was the possible need to terminate MIKEY in the UICC and/or terminal in the combined method. The use of MIKEY relates to the PTP delivery of a key~~

End of third change