3GPP TSG-SA-WG3 Meeting #32
9th – 13rd February 2004, Edinburgh, GB

Tdoc ⌘S3-040088

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.246 CR CRNum** ⌘**rev** ⌘ Current version: 1.0.0 ⌘

*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:	⌘	CR on MBMS key Management procedures
Source:	⌘	AXALTO, Gemplus, Oberthur
Work item code:	⌘	MBMS
Date:	⌘	02/02/2004
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:	⌘	MBMS key management has not been specified
Summary of change:	⌘	UICC-based solution as MBMS key management
Consequences if not approved:	⌘	.

Clauses affected:	⌘	6

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

Other comments:	⌘	

********FIRST CHANGE**********

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[4] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

[5] 3GPP TS 22.246: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Stage 1; MBMS User Services".

[6] 3GPP TS 31.115: “3rd Generation Partnership Project; Technical Specification Group Terminals; Secured packet structure for (U)SIM Toolkit applications”.

[7] 3GPP TS 31.116: “3rd Generation Partnership Project; Technical Specification Group Terminals; Remote APDU Structure for (U)SIM Toolkit applications”.

********END OF FIRST CHANGE**********

********SECOND SET OF CHANGES**********

6 Security mechanisms

6.1 Authentication and authorisation of a user

Editor's note: This section will contain the details of how a user joins a particular Multicast Service.

6.2 Key update procedure

6.2.1 Overview

The multicast data of a specific MBMS service is protected by a symmetric key (Short Term key SK). SK is derived from a high level key (i.e. Broadcast Access key- BAK), which is securely stored in the UICC.

BAK keys are never revealed in clear outside the UICC but are used with the appropriate security functions to derive the encryption keys SK (see Protection of the transmitted traffic section). BAK keys are common to all the subscribers of a particular MBMS bearer service. Hence, for security reasons, they should be renewed quiet often (e.g. once a month).

BAK keys are distributed to the UICC prior to service by the MBMS keys administrative procedures described in the following chapter.

MBMS Registration keys (RK) are used to protect BAK delivery to the UICC. RK may be different for each subscriber.

Note: RK provision is out of the scope of this document and may likely be performed at personalization stage or by remote management.

6.2.1 Administrative procedures

The BMSC is responsible to update the BAK keys of the UEs which are subscribed to a particular MBMS bearer service before that the particular updated BAK is used. The mechanisms to perform these key updates are described in the following subsections distinguishing three different cases: non-roaming case, roaming case and UE initiated key updates.

Note: These administrative procedure does not apply exclusively to the BAK values but to any MBMS data related to a particular MBMS bearer service which is stored in the UICC (e.g. MBMS_ID)

6.2.1.1 Non Roaming Case:

The UICC is provisioned with several MBMS key sets to store BAK keys and several files containing other MBMS related data (e.g. MBMS_ID, BAK_Expiration,…)

For each MBMS key set a Registration key (RK) is provisioned in the UICC.

In non-roaming case, RK is always known by the HN.

When the BMSC request a MBMS Administrative Procedure it uses the Remote APDU for (U)SIM Toolkit applications as defined in [7] and the security mechanisms defined in [6] to perform the MBMS key/file remote management to the UICC. These security mechanisms provide authentication, message integrity, replay detection, sequence integrity and message confidentiality.

Editor's Note: Interfaces between BMSC and UICC is not to be further standardised as it is already done for any application resident in or behind the 3G.

The following flow shows this procedure:

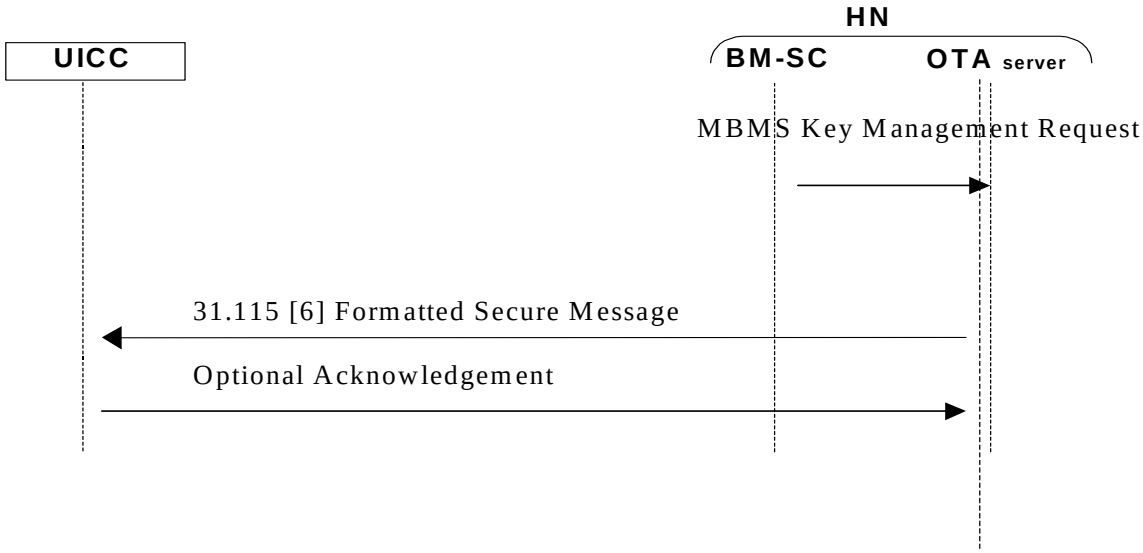


Figure 2: Key Administrative procedure to the UICC. Non-roaming case.

6.2.1.2 Roaming case:

This case is similar to the previous one, but the initiative to perform the key administrative procedure corresponds to a visited BMSC. In this case, the visited BMSC shall contact the Home BMSC of the subscriber in roaming to perform a key Management Request on his behalf. Additionally, It is possible that RK that is used for encrypting the BAK values of the visited BMSC, is not known by the Home Network.

Note: RK used in roaming case may correspond to a different key set in the UICC of those used in the non-roaming case.

Note: The mechanisms to provide RK confidentiality between the Home and Visited PLMNs is out of the scope of this specification and may likely involved the presence of a Third Trusted Party.

The Home BMSC may then proceed with the MBMS key Management Request as in the previous case, using MBMS data received by the Visited BMSC. That may include eventually encrypted BAK values and any other attached information (e.g. MBMS_ID, BAK_Expiration,…).

Editor's Note: The exact content of the message between visited and home BMSC is to be standardised by the corresponding groups of 3GPP

The following data flow shows this procedure:

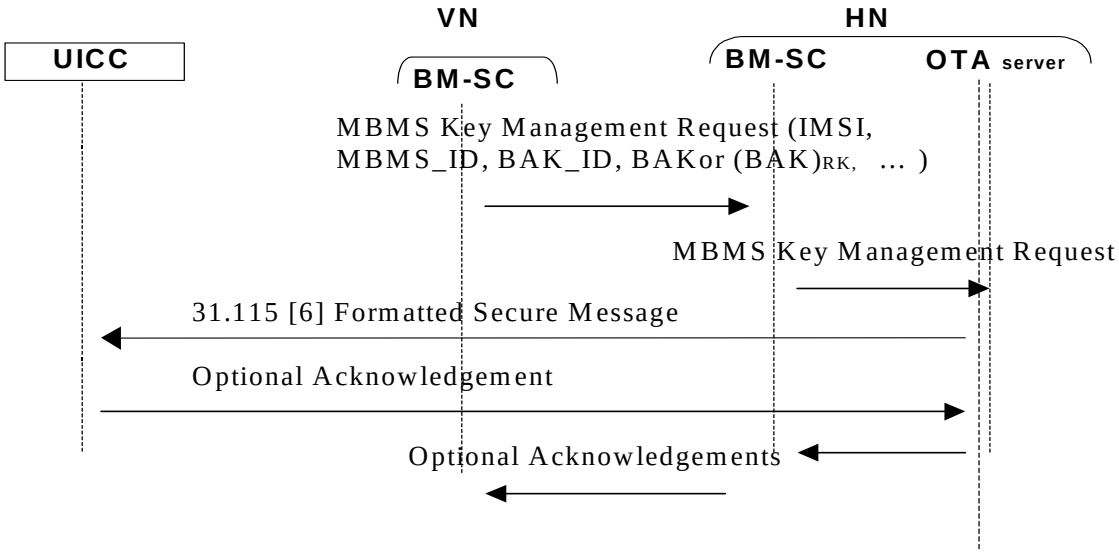
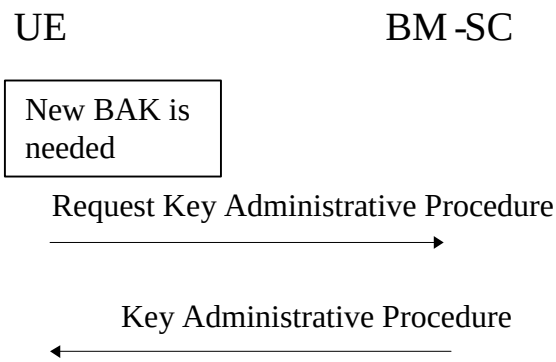


Figure 3: Key Administrative procedure to the UICC. Roaming case.

6.2.1.3 UE Initiated Request

Once a UE has joined a multicast service, the ~~UE~~ ME ~~should~~ may fail to~~try to~~ get the ~~high~~ low level key (SK) that will be used to 'protect' the data transmitted as part of this multicast service (e.g. the user's UICC has not a correct BAK corresponding to this service). The ME may notice this by inspecting the MBMS related files in the UICC. Alternatively this can be indicated by the UICC once failing to derive the SK corresponding to the MBMS service. ~~If the UE fails to get hold of this key or receives confirmation that no updated key is necessary or available at this time, then, unless the UE has a still valid, older key, the UE shall leave the MBMS user service.~~ The UE may then try~~tries~~ to ~~get~~ request a MBMS key management request to the BMSC (e.g. asking for a new BAK) ~~the high level key~~ using the ~~second~~ first message in the below flow.

~~The BM-SC controls when the high level keys used in a multicast service are to be changed. The flow in figure 2 describes how the high level key changes are performed.~~



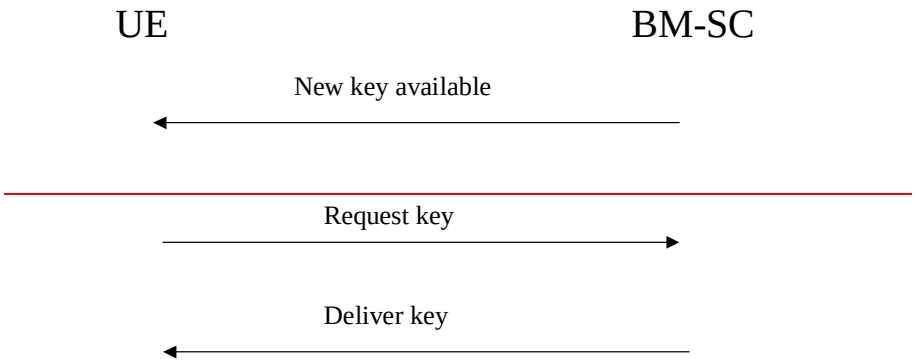


Figure 42: UE initiated Key Management Requesthigh-level key changes

~~The first message is sent out by the BM-SC to indicate that new keys are available. It is an optional message in the flow. If it is sent to all UEs, then it needs to be ensured that all the UEs do not request the new key simultaneously.~~

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

Editor's Note: It is FFS the list of reasons to be indicated in this request. A non exhaustive list may be the following:

-MBMS_ID not subscribed; BAK_ID not present; SK_RAND antireplay error; SK Counter exceeds.

After receiving the ~~second~~ request key message the BM-SC should send out the appropriate key management procedure ~~request~~ to the UICC~~E~~ as described in the previous two cases~~protected by the relevant means.~~ Upon successfully receiving the new key, the ~~UE~~ ME may retry to ask the UICC for the corresponding SK ~~should store this key for later use~~.

If the UE fails to get the key management procedure after some delay, the UE shall leave this MBMS service or retry the UE initiated request procedure.

~~Editor's note: MIKEY is being considered as the method for carrying keys. 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.~~

6.32 Protection of the transmitted traffic

The data transmitted to the UEs is protected by a symmetric key (SK) that is shared by the BM-SC and UEs that are accesing the MBMS service. The protection of the data is applied by the BM-SC. In order to determine which key was used to protect the data a ~~Key~~SK_ID is included with the protected data. The ~~Key~~SK_ID will uniquely identify the high-level key and contain other information needed to calculate the low-level keys. SK_ID is composed of the following fields (MBMS_ID | BAK_ID | SK_RAND) where :

-MBMS_ID : Identifying the MBMS bearer service.

Editor's note: Naming to be checked against SA2 discussion for MBMS bearer identifiers

-BAK_ID : Identifying the high level key (BAK) to be used to derive the SK

-SK_RAND: Including additional material to derive SK

Editor's note: It is FFS the content of SK_RAND e.g. to provide antireplay protection mechanisms.

NOTE: Including the ~~Key~~SK_ID with the protected data stops the UE trying to decrypt and render content for which it does not have the correct key.

The flow in figure 5~~3~~ shows how the protected content is delivered to the UE.

Figure ~~3~~5: Protected content delivery to the UE

If the ME does not have the low level key SK, identified by the SK_ID, then it shall ask the UICC to retrieve it using the SK_ID information and the stored high-level key (BAK) corresponding to the MBMS_ID and BAK_ID pairs, as shown in the following figure:

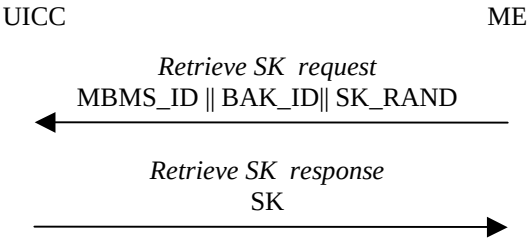


Figure 6: SK retrieval from the UICC

The UICC will first search the BAK corresponding to the MBMS_ID, BAK_ID pair. Then, the UICC computes SK
SK= f_{MBMS} (BAK || SK_RAND)

Editors Note: Mechanisms for antireplay protection in f_{MBMS} are FFS.

Editor's Note: The exact definition of f_{MBMS} needs to be standardised by 3GPP

If the ~~UE~~ UICC does not have the high level key (BAK) indicated by ~~Key~~SK_ID, then it shall indicate it to the ME with a corresponding status conditioned. The UE~~it~~ should then fetch the high level key using the methods discussed in the previous clause.

After using a key to decrypt protected traffic, the UE deletes any older key for this multicast service.

Editor's note: This section may contain several protection methods.

Editor's note: If SRTP is chosen, the master key identifier can be used to indicate the current MBMS key whichever key management method is chosen.
