

CR-Form-v7

CHANGE REQUEST

⌘ **33.246 CR 005** ⌘ rev **3** ⌘ 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 ME Radio Access Network Core Network

Title:	⌘ Clean up of MBMS TS		
Source:	⌘ SA WG3		
Work item code:	⌘ MBMS	Date:	⌘ 15/11/2004
Category:	⌘ D	Release:	⌘ Rel-6
	Use <u>one</u> 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 <u>one</u> 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:	⌘ Editorial clean up of MBMS TS		
Summary of change:	⌘ Editorial clean up and editorial clarifications of MBMS TS		
Consequences if not approved:	⌘		

Clauses affected:	⌘ Introduction, 1, 3.2, 3.3, 4.1, 5.3, 6.4.4, 6.4.6.1, 6.4.6.2, 6.5.4, 6.6.1										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications ⌘ Test specifications ⌘ O&M Specifications ⌘	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
Other comments:	⌘										

***** NEXT CHANGE*****

Introduction

The security of MBMS provides different challenges compared to the security of services delivered over point-to-point services. In addition to the normal threat of eavesdropping, there is also the threat that it may not be assumed that valid subscribers have any interest in maintaining the privacy and confidentiality of the communications, and they may therefore conspire to circumvent the security solution (for example one subscriber may publish the decryption keys enabling non-subscribers to view broadcast content). Countering this threat requires the decryption keys to be updated frequently in a manner that may not be predicted by subscribers while making efficient use of the radio network.

1 Scope

The Technical Specification covers the security procedures of the Multimedia Broadcast/Multicast Service (MBMS) for 3GPP systems (UTRAN and GERAN). MBMS is a ~~GPRS~~ 3GPP system network bearer service over which many different applications could be carried. The actual method of protection may vary depending on the type of MBMS application.

***** NEXT CHANGE*****

3.2 Symbols

For the purposes of the present document, the following symbols apply:

~~MUK_I Integrity key derived from key MUK~~
~~MUK_C Confidentiality key derived from key MUK~~
~~MSK_I Integrity key derived from key MSK~~
~~MSK_C Confidentiality key derived from key MSK~~

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

MBMS	Multimedia Broadcast/Multicast Service
MGV-F	MBMS key Generation and Validation Function
MGV-S	MBMS key Generation and Validation Storage
<u>MRK</u>	<u>MBMS Request Key</u>
<u>MSK</u>	<u>MBMS Service Key</u>
<u>MSK_C</u>	<u>Confidentiality key derived from key MSK</u>
<u>MSK_I</u>	<u>Integrity key derived from key MSK</u>
<u>MTK</u>	<u>MBMS Traffic Key</u>
<u>MUK</u>	<u>MBMS User Key</u>
<u>MUK_C</u>	<u>Confidentiality key derived from key MUK</u>
<u>MUK_I</u>	<u>Integrity key derived from key MUK</u>
<u>NAF</u>	<u>Network Application Function</u>

***** NEXT CHANGE *****

4.1 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3GPP system. A requirement of a multicast service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a multicast service. ~~The AKA protocol (see TS 33.102 [4]) is~~

~~used to both authenticate a user and agree on keys to be used between that user and the network. These keys are subsequently used to provide protection of traffic between the network and the UE.~~



Figure 4.1: MBMS security architecture

Figure 4.1 gives an overview of the network elements involved in MBMS from a security perspective. Nearly all the security functionality for MBMS (beyond the normal network bearer security) resides in either the BM-SC or the UE.

The Broadcast Multicast – Service Centre (BM-SC) is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission. It is responsible for generating and distributing the keys necessary for multicast security to the UEs and for applying the appropriate protection to data that is transmitted as part of a multicast service. The BM-SC also provides the MBMS bearer authorisation for UEs attempting to establish multicast bearer.

The UE is responsible for receiving or fetching keys for the multicast service from the BM-SC and also using those keys to decrypt the MBMS data that is received.

***** NEXT CHANGE *****

5.3 Protection of the transmitted traffic

The traffic for a particular MBMS service may require some protection depending on the sensitivity of the data being transmitted (e.g. it is possible that the data being transmitted by the MBMS service is actually protected by the DRM security method and hence ~~might not require~~ no additional protection. However, MBMS protection is independent of DRM protection). This protection will be either confidentiality and integrity or just confidentiality. The protection is applied end-to-end between the BM-SC and the UEs and will be based on a symmetric key shared between the BM-SC and the UEs that are currently accessing the service. The actual method of protection specified may vary depending on the type of data being transmitted, e.g. media streaming application or file download.

NOTE: When MBMS data is received over a point-to-point MBMS radio bearer, it would be ciphered between the BM-SC and UE and may also ciphered over the radio interface. This “double ciphering” is unnecessary from a security point of view and hence the decision of whether or not to apply radio interface ciphering to a point-to-point MBMS radio bearer is outside the scope of this specification.

***** NEXT CHANGE *****

6.4.4 General extension payload

The MSK and MTK shall be delivered in messages that conform to the structure defined in RFC 3830 [9] (MIKEY). To be able to keep track of the keys, a new general Extension Payload (EXT) is defined that conforms to the structure defined in section 6.15 of RFC 3830 [9] (MIKEY). The IDs of the involved keys are kept in the EXT, to enable the UE to look up the identity of the key which was used to protect the message, and which key is delivered in the message. This EXT is incorporated in the MIKEY messages (see Figure 6.4). When an MSK is delivered to a UE, the MIKEY message contains an EXT that holds the MUK ID of the MUK used to protect the delivery, and the MSK ID of the MSK delivered in the message. For messages that contain an MTK, the EXT contains the MSK ID of the MSK used to protect the delivery, and the MTK ID of the MTK contained in the message. The MSK ID and MTK ID are increased by 1 every time the corresponding key is updated. It is possible that the same MTK is delivered several times in multicast, and the ME can then discard messages related to a key it already has instead of passing them to the MG-V-F.

The MG-V-F (see clause 6.5) protects itself from a possibly malicious ME by checking the integrity and freshness of the MIKEY message.

The format of the key IDs shall be represented by unsigned integer counters, different from zero. The reason for disallowing zero is that it is reserved for future use. Note that this means that there can only be $2^n - 1$ different keys in use during the same session, where n is the number of bits in the ID field.

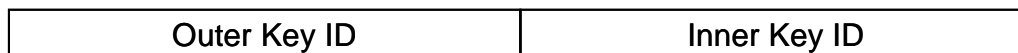


Figure 6.4: Extension payload used with MIKEY

The Inner Key ID is the ID of the key that is transported in the message (i.e. an MSK or MTK). The Outer Key ID is the ID of the key used as pre-shared secret for the key delivery (i.e. an MUK or MSK).

***** NEXT CHANGE *****

6.4.6.1 MSK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MSK delivery, the MUK ID is extracted from the Extension Payload.
2. The Timestamp Payload is checked, and the message is discarded if the counter [in the Timestamp Payload](#) is [larger-smaller](#) or equal to the [current MIKEY-stored](#) replay counter associated with the given MUK (the [stored replay](#) counter value is retrieved from MGVS). To avoid issues with wrap around of the ID fields ``smaller than`` should be in the sense of RFC1982 [10].
3. The Security Policy payload is stored if it was present.
4. The message is transported to MGVS-F for further processing, cf 6.5.2.
5. The MGVS-F replies success or failure.

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MTSK delivery, the MSK ID is extracted from the Extension Payload.
2. The Timestamp Payload is checked, and the message is discarded if the counter [in the Timestamp Payload](#) is [larger-smaller](#) or equal to the [current MIKEY-stored](#) replay counter associated with the given MSK (the [stored replay](#) counter value is retrieved from MGVS). To avoid issues with wrap around of the ID fields ``smaller than`` should be in the sense of RFC1982 [10].
3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message shall be discarded.
4. The message is transported to MGVS-F for further processing, cf 6.5.3.
5. The MGVS-F replies success (i.e. sending the MTK) or failure.

***** NEXT CHANGE *****

6.5.4 MTK validation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC as defined in RFC 3830 [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. If the MAC verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the MAC verification is successful, then the MGV-F shall update SEQs with SEQp value and start the generation of MTK. The MGV-F provides the MTK to the ME.

If MAC verification is successful, the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of RFC 3830 [9] (MIKEY).

***** NEXT CHANGE *****

6.6.1 General

The data transmitted to the UEs is protected by a symmetric key (an MTK) that is shared by the BM-SC and UEs that are accessing 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 key identification information is included with the protected data. The [key identification information](#) **Key_ID** will uniquely identify the MSK and ~~contain other information needed to calculate the~~ MTK. The MTK is ~~derived-processed~~ according to the methods described in subclauses 6.4 and 6.5. Whenever data from an MBMS User Service has been decrypted, if it is to be stored on the UE it will be stored decrypted.

NOTE: Including the key identification information with the protected data stops the UE trying to decrypt and render content for which it does not have the MSK.