

CR-Form-v7

## CHANGE REQUEST

**33.246 CR 028 rev 1** 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

<b>Title:</b>	Shorter MKI		
<b>Source:</b>	SA WG3		
<b>Work item code:</b>	MBMS	<b>Date:</b>	23/11/2004
<b>Category:</b>	<b>C</b>	<b>Release:</b>	Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		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)

<b>Reason for change:</b>	MKI field is too long, and contains unnecessary information. Also Section 6.6.2.2 is unclear in the sense that it gives the impression that the MKI needs to be globally unique. This is not the case; it only needs to be unique in any given SRTP context. The Network ID is known once the SRTP context is identified.
<b>Summary of change:</b>	Removed the Network ID from the MKI field.
<b>Consequences if not approved:</b>	The MKI will contain information that is not required for functionality and there will be a waste of bandwidth.

<b>Clauses affected:</b>	6.6.2.1, 6.6.2.2										
<b>Other specs affected:</b>	<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	
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
		Test specifications									
		O&M Specifications									
<b>Other comments:</b>											

## 6.6.2 Protection of streaming data

### 6.6.2.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in RFC 3711 [11] shall be used. The MTK is carried to the UEs from the BM-SC using RFC 3830 [9] (MIKEY) with extensions defined according to this specification. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in section 4.3 of RFC 3830 [9]. The correct MTK to use to decrypt the data is indicated using the MKI (Master Key identifier) field, which is included in the SRTP packets as defined in RFC 3711 [11]. The form of MKI shall be a concatenation of ~~Network ID~~, Key Group ID, MSK ID and MTK ID, i.e. MKI = (~~Network ID~~ || Key Group ID || MSK ID || MTK ID).

If the SRTP packets are to be integrity protected, the SRTP authentication tag is appended to the packets as defined in RFC 3830 [9].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in section 6.10.1 in RFC 3830 [9].

### 6.6.2.2 Packet processing in the UE

When the SRTP module receives a packet, it will [retrieve the correct cryptographic context identified by destination transport address, destination port and SSRC \(according to RFC 3711\)](#), check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

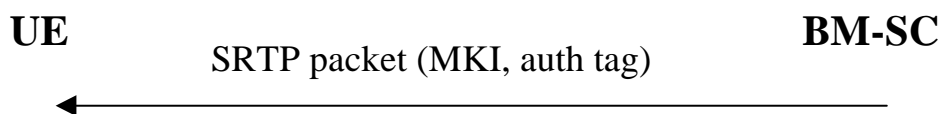
**NOTE:** [The cryptographic context needs to be unique for each SRTP stream.](#)

**NOTE:** The SRTP module does not need to interpret the MKI field semantics. It only checks whether it has the MTK corresponding to the MKI value.

If the check is successful, the SRTP module processes the packet according to the security policy.

If the SRTP module does not have the MTK, it will request the MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, the SRTP module will derive new session keys from the MTK and process the packet. However, if the key management module does not have the MSK indicated by MKI, then it should fetch the MSK using the methods discussed in the clause 6.3.

The below flow shows how the protected content is delivered to the UE.



**Figure 6.8: Delivery of protected streaming content to the UE**