3GPP TSG-SA WG3 Meeting S3#35
St Paul's Bay, Malta, October 5-8, 2004

Tdoc ⌘S3-040818

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**020**	⌘**rev**	**-**	⌘	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:	⌘	MTK update procedure for streaming services		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	28/09/2004
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	It is not specified how the MTK is transprted to the UE in streamingn services
Summary of change:	⌘	MTK is interleaved with the RTP traffic and separated with UDP port number
Consequences if not approved:	⌘	It will remain unspecified how the MTK is delivered in streaming services.

Clauses affected:	⌘	6.3.3, 6.6.2				
		Y	**N**			
Other specs Affected:	⌘	**Y**		Other core specifications	⌘	26.346
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

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

6.3.3.2 MTK update procedure in streaming services

The MTK ~~is~~ shall be delivered to the UE as in 6.3.2.3.1 but the MIKEY ACK ~~is~~ shall not be used. MIKEY messages transporting MTKs shall be interleaved with the RTP traffic using the same IP address as the RTP traffic. MIKEY messages shall be transported to UDP port number specified for MIKEY.

Editor's Note: The UDP port number needs to be specified for MIKEY.

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

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 [11] shall be used. The MTK is carried to the UEs from the BM-SC using MIKEY [9] 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 chapter 4.3 of [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 [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 [9].

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

6.6.2.2 Packet processing in the UE

When the SRTP module receives a packet, it will check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

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 subclause 6.3.

If the correct MTK is not present in the UE when RTP traffic arrives, the UE shall wait for the next MTK update procedure from the BM-SC as described in 6.3.3.2.

NOTE: It is implementation specific issue whether the UE spools encrypted packets or discards all packets before the UE has received the correct MTK.

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

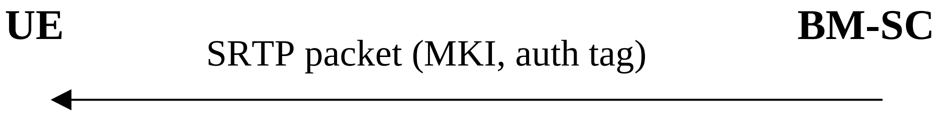

Figure 6.8: Delivery of protected streaming content to the UE