3GPP TSG-SA WG3 Meeting S3#37
Sophia, France, 21-25 February, 2005

Tdoc* ⌘*S3-050135

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**045**	⌘**rev**	**1**	⌘ Current version:	**6.1.0** ⌘

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:	⌘ Usage of security policy payload			
Source:	⌘ SA WG3			
Work item code:	⌘ MBMS		***Date:***	⌘ 22/2/2005
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:	⌘	Current TS specifies that CS ID map info is present in MTK messages in streaming services to carry the ROC for SRTP, but according to RFC 3830 SP (Security Policy) payload should be also present in this case. However, SP payload is not needed since it is carried in MSK level messages. It is proposed that CS ID Map info is optionally carried, but SP payload is not carried in MTK messages. Also, it is not clear in the TS when SP payload is delivered to the UE and if it is needed for download services since all required parameters are signalled outside of MIKEY. It is proposed that it is mandatory to the BM-SC to send the SP payload when the MSK delivery was triggered by the MSK request procedure and MBMS User Service Registration, otherwise the use of the SP payload in MSK messages is optional.
Summary of change:	⌘	The SP payload is not present in MTK messages although CS ID map info is present. The BM-SC may decide when to attach CS ID map info to MTK messages. It is mandatory to the BM-SC to send the SP payload when the MSK delivery was triggered by MSK request procedure, otherwise the use of SP payload in MSK messages is optional. It is clarified that SP payload is not needed for download services.
Consequences if not approved:	⌘	Unclear usage of SP payload.

Clauses affected:	⌘	6.4.2, 6.4.5.1, 6.4.5.3, 6.6.2.2			
		Y	N		
Other specs Affected:	⌘		N	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

6.4.2 MIKEY common header

MSKs shall be carried in MIKEY messages. The messages are sent point-to-point between the BM-SC and each UE. The messages use the MUK shared between the BM-SC and the UE as the pre-shared secret in MIKEY.

Once the MSK is in place in the UE, the UE can make use of the multicast MTK messages sent by the BM-SC. The MTK is carried in messages conforming to the structure defined by MIKEY and use the MSK as the pre-shared secret.

If the BM-SC requires an ACK for an MSK key update message this is indicated by setting the V-bit in the MIKEY common header. The UE shall then respond with a MIKEY message containing the verification payload. In the case the server does not receive an ACK, normal reliability constructions can be used, e.g., start a timer when the message is sent and then resend the message if no ACK is received before the timer expires.

The CSB ID field of MIKEY common header is not used.

In case of download services, the SP payload is not used and CS ID map type is set to value ‘1’ as defined in [16]. In case of streaming services the CS ID map type is set to value ‘0’ as defined in RFC 3830 [9]

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

6.4.5.1 MSK message structure

The structure of the MIKEY message carrying a MSK key is depicted in Figure 6.5. The actual key that is delivered is kept in the KEMAC payload. The MIKEY-RAND is used to derive e.g. encryption and authentication keys from the received keys. It is sent in all the MSK delivery messages. The identity payloads of the initiator's and responder's IDs shall be included in the MSK transport messages. IDi is the ID of the BM-SC (i.e. NAF-ID) and IDr is the ID of the UE's username (i.e.B-TID). Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. The SP payload is used only with streaming services. The BM-SC shall ensure that the UE has received the SP payload before the SP payload needs to be applied in the streaming service. The BM-SC shall include the SP payload when the MSK delivery was triggered by the UE using the MSK request procedure or the MBMS User Service Registration procedure, otherwise it is optional for the BM-SC to include the SP payload into MSK delivery messages. The Key Validity Data subfield is present in the KEMAC payload when MSK is transported but it is not present for MTK transport. The field defines the Key Validity Time for MSK in terms of sequence number interval (i.e. lower limit of MTK ID and upper limit of MTK ID). The lower limit of the interval defines the SEQs to be used by the MGV-F (see clause 6.5).

~~Editor's Note: The contents of the Security Policy payload depends on the used security protocols. RFC 3830 [9] (MIKEY) has defined Security Policy payload for SRTP, but for other security protocols there is a need to define new Security Policy payloads. The exact definitions of these are FFS.~~

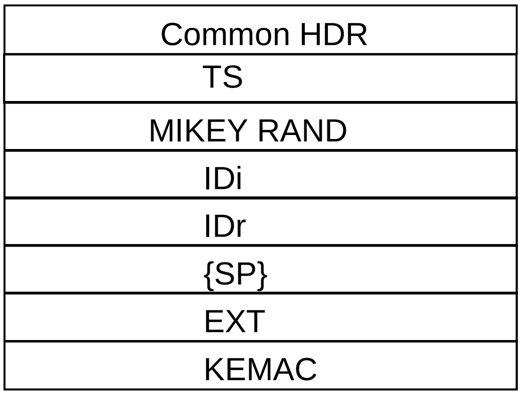

Figure 6.5: The logical structure of the MIKEY message used to deliver MSK. For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

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

6.4.5.3 MTK message structure

The structure of the MIKEY message carrying a MTK key is depicted in Figure 6.7. The actual key that is delivered is kept in the KEMAC payload. If MTK is to be used for streaming protection, then a 112 bit salt shall be added to the KEMAC payload in addition to the MTK. The network identity payloads (IDi) shall be used in MTK transport messages. It is optional for the BM-SC to include the current ROC-value within the CS ID map info payload of the MIKEY common header payload in an MTK message. In this case the Policy_no_i and SSRC_i fields should be set to zero by the sender and shall be ignored by the receiver. The SP payload shall not be included in MTK messages.

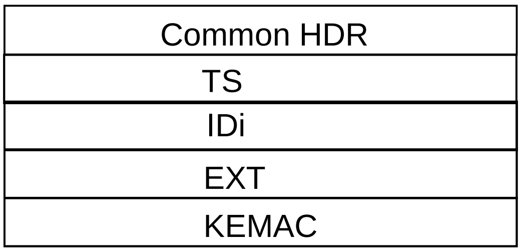

Figure 6.7: The logical structure of the MIKEY message used to deliver MTK

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

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 [11]), check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

NOTE 1: The cryptographic context needs to be unique for each SRTP stream.

NOTE 2: 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.

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 clause 6.3.3.2.

NOTE 3: It is implementation specific issue whether the UE spools encrypted packets or discards all packets before the UE has received the correct MTK.

If the SRTP module has lost synchronisation on the ROC (Roll-over counter) of the SRTP stream, it shall wait for the next MTK update message received within the ptm stream. ~~The BM-SC shall deliver the current ROC-value within the CS ID map info payload of the MIKEY common header payload.~~

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

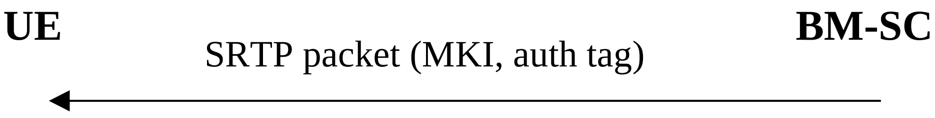

Figure 6.8: Delivery of protected streaming content to the UE