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

Tdoc ⌘S3-050114

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **043** ⌘ **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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Alignment according to MIKEY related IETF work
Source:	⌘	SA WG3
Work item code:	⌘	MBMS
Date:	⌘	14/2/2005
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:	⌘	MIKEY IETF draft has been updated.
Summary of change:	⌘	Removed some editor's notes about pending IETF work and added UDP port number for MIKEY.
Consequences if not approved:	⌘	TS is not aligned with IETF draft

Clauses affected:	⌘	2, 6.3.3.2.2, 6.4.1, 6.4.4

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

Other comments:	⌘	

******* NEXT 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: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246: "MBMS User Services".

[6] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[7] 3GPP TS 31.102: "Characteristics of the USIM application".

[8] IETF RFC 2617 "HTTP Digest Authentication".

[9] IETF RFC 3830 "MIKEY: Multimedia Internet KEYing"

[10] IETF RFC 1982 "Serial Number Arithmetic".

[11] IETF RFC 3711 "Secure Real-time Transport Protocol".

[12] 3GPP TS 43.020: "Security related network functions".

[13] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service; Protocols and Codecs".

[14] 3GPP TS 33.210: "Network domain security; IP network layer security".

[15] OMA-DRM-DCF-v2_0: "OMA DRM Content Format", www.openmobilealliance.org

[16] IETF internet draft: "The Key ID Information Type for the General Extension Payload in MIKEY" <draft-~~carrara~~msec-newtype-keyid-0~~0~~1.txt>.

[xx] Port numbers at IANA, http://www.iana.org/assignments/port-numbers

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

6.3.3.2.~~1~~2 MTK delivery in streaming

MIKEY messages transporting MTKs shall be sent 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 *******

6.4.1 General

MIKEY is used to transport the MSKs and MTKs from the BM-SC to the UE. Clauses 6.4.2, 6.4.3, 6.4.4 and 6.4.5 describe how to create the MIKEY messages, while clause 6.4.6 describes the initial processing by the ME on these messages. The final processing is done by the MBMS key Generation and Validation Function (MGV-F) and is described in clause 6.5.

MIKEY shall be used with pre-shared keys as described in RFC 3830 [9]. The UDP port number for MIKEY is 2269 [xx]

To keep track of MSKs and MTKs, a new Extension Payload (EXT) [16] is added to MIKEY. The Extension Payload can contain the key types and identities of MSK and the MTK and Key Domain ID (see clauses 6.3.2 and 6.3.3).

******* 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 key that is derived in the message, a general Extension Payload (EXT) with Type field value x is used that conforms to the structure defined in reference [16].

Editor's Note: The type value will be replaced by value requested from IANA.

The EXT includes a Key Domain ID and one or two Key Type ID sub-payloads depending on the message. These are used as follows.

For MSK delivery the EXT includes the Key Domain ID and a Key Type ID sub-payload. The Key Domain ID has the value as specified in clause 6.3.2.1. The Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MSK ID, see figure 6.4a. The key that is used to protect the message, i.e. MUK, is identified as specified in clause 6.1.

For MTK delivery the EXT includes the Key Domain ID and two Key Type ID sub-payloads. The Key Domain ID has the value as specified in clause 6.3.2.1. The first Key Type ID sub-payload includes the type and ID of the key that is used to protect the message, i.e. the MSK ID, and the second Key Type ID sub-payload includes the type and ID of the key that is delivered in the message, i.e. the MTK ID, see figure 6.4b.

~~Editor's Note: The Key Domain ID needs to be added to [16]. It may need an extension payload type of its own.~~

See~~.~~ clauses 6.3.2.1 and 6.3.3.1 for definition of MSK ID and MTK ID. The MTK ID is increased 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 MGV-F.

The MGV-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 integers, 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.

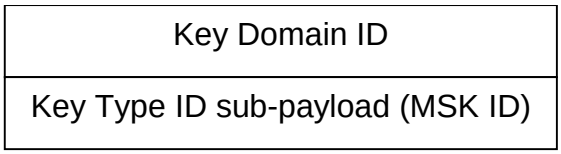

Figure 6.4a: Extension payload used with MIKEY MSK message

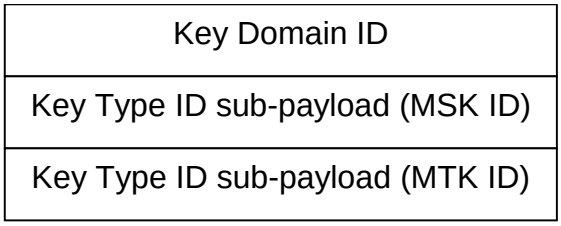

Figure 6.b: Extension payload used with MIKEY MTK message