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

Tdoc ⌘S3-040800

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **013** ⌘ **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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Adding MIKEY payload type identifiers
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	27/09/2004
Category:	⌘	**F**
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:	⌘	Unspecified identifiers for several MIKEY MBMS payloads
Summary of change:	⌘	Add identifier values from the private name space (draft-ietf-msec-mikey-08 clause 10) which may later be replaced by IANA requested values if they can be obtained on time.
Consequences if not approved:	⌘	Implementations will not know what identifier to use or receive for various MIKEY MBMS payloads.

Clauses affected:	⌘	6.4.4, new clauses (6.4.5.0, 6.4.5.1.1, 6.4.5.3.1)
Other specs affected:	⌘	Y / N [ ] / N Other core specifications [ ] / N Test specifications [ ] / N O&M Specifications
	⌘	
Other comments:	⌘	

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).

For MBMS the general extension payload (according to table 6.15 of [9]) shall be identified by following private value:

Type	Value	Comments
3GPP MBMS	241	3GPP extension payload for MBMS key management

Editor's Note: The type value may be replaced by an IANA requested value.

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 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 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.

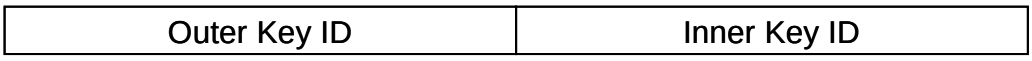

Figure 6.4: Extension payload used with MIKEY

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).

6.4.5 MIKEY message structure

6.4.5.0 MSK and MTK transport identification

For MBMS the MIKEY common header data type field (cf. Table 6.1a of clause 6.1 [9]) identifies the type of key that is transported.

The transport of MSK and MTK transport shall be identified by following private values:

Data type	Value	Comment
MSK	241	Transport of MSK encrypted with MUK
MTK	242	Transport of MTK encrypted with MSK

Editor's Note: The type values may be replaced by IANA requested values.

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 only in the initial MSK delivery message. 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 and IDr is the ID of the UE. Security Policy (SP) payload includes information for the security protocol such as algorithms to use, key lengths, initial values for algorithms etc. 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 type (URI or NAI) of identity payloads to use are for further study.

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.

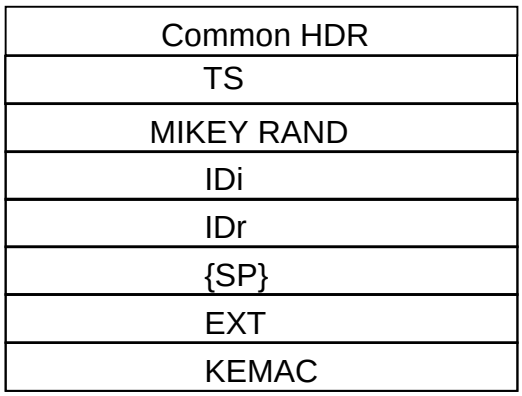

Figure 6.5: The logical structure of the MIKEY message used to deliver MSK. For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

6.4.5.1.1 Key Data Sub payloads carried by KEMAC

For MBMS MSK transport, the Key Data Sub payload (cf. clause 6.13 of [9]) that is carried by the KEMAC payload shall be identified by following private value:

Data type	Value	Comment
MSK	241	MSK encrypted with MUK

Editor's Note: The type value may be replaced by an IANA requested value.

6.4.5.2 MSK Verification message

If the BM-SC expects a response to the MSK-transport message (i.e., the V-bit in the MIKEY common header is equal to 1), the UE shall send a verification message as a response. The verification message shall be constructed according to section 3.1 of MIKEY, and shall consist of the following fields: HDR || TS || IDi_ || IDr || V, where IDi is the ID of the BM-SC and IDr is the ID of the UE. Note that the MAC included in the verification payload, shall be computed over

both the initiator's and the responder's IDs as well as the timestamp in addition to be computed over the response message as defined in RFC 3830 [9]. The key used in the MAC computation is the MUK_I.

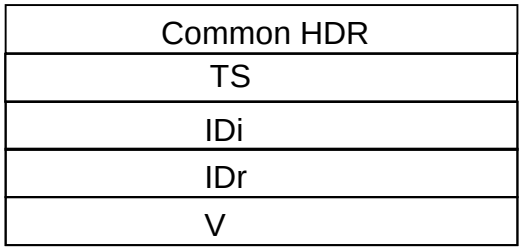

Figure 6.6: The logical structure of the MIKEY Verification message

The verification message shall not be sent as a response to MIKEY messages delivering MTK.

The verification message shall be constructed by the ME, except for the MAC field, and then be given to the MGV-F that will perform the MAC computation and will return the verification message appended with the MAC to the ME. The ME shall send the message to the BM-SC.

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. The network identity payloads (IDi) shall be used in MTK transport messages.

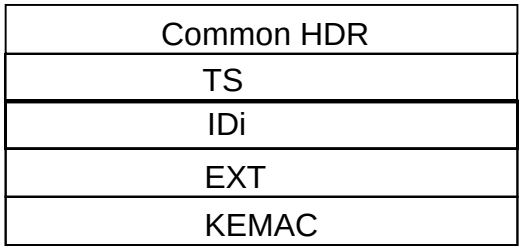

Figure 6.7: The logical structure of the MIKEY message used to deliver MTK

6.4.5.3.1 Key Data Sub payloads carried by KEMAC

For MBMS MTK transport, the Key Data Sub payload (cf. clause 6.13 of [9]) that is carried by the KEMAC payload shall be identified by following private value:

Data type	Value	Comment
MTK	242	MTK encrypted with MSK

Editor's Note: The type value may be replaced by an IANA requested value.