3GPP TSG SA WG3 Security — S3#32 **S3-040081**

9 - 13 February 2004

Edinburgh, UK

Title: **Use of MIKEY in the Combined method**

Source: **Nokia**

Document for: **Discussion and decision**

Agenda Item: **6.20**

Work Item: **MBMS**

1 Introduction

The general message flow of the Combined method was presented in [S3-030751]. This discussion paper presents a key delivery of the Combined method in more detail. The key delivery can be based on MIKEY protocol, which is specified in [MIKEY]. MIKEY protocol is enhanced so that it can be used to deliver TEKs (traffic encryption keys) and BAKs (broadcast access keys) in encrypted form. The enhancements are designed so that:

- Minimal amount of payloads are used i.e. bandwidth is conserved.
- Enhancements do not prevent the original use of MIKEY.
- Minimal extensions to MIKEY

The needed enhancements are highlighted using **bold** style.

2 Assumptions

The assumptions are the following:

- The service announcement defines the security policy i.e. used algorithms are explicitly defined in service announcement.
- Crypto Session Bundle ID (CSB ID) and IDi identify the service.

3 Notation

The following notation is used in the following sections:

[] an optional piece of information

{} denotes zero or more occurrences

HDR header

T timestamp payload

IDx ID payload

SP security policy payload

KEMAC key data transport payload

V verification message payload

MBMSKEY MBMS key data transport payload

4 BAK Delivery

The BAK delivery can be based on MIKEY TGK re-keying and CSB updating with pre-shared keys.

The MIKEY TGK re-keying with pre-shared keys has the following messages:

1. The initiator sends: HDR, T, [IDi], {SP}, KEMAC

   Timestamp payload (T) is used to provide anti-replay protection, ID payload is used to identify peer, security policy payload (SP) is used to provide security parameters and key data transport payload (KEMAC) contains key(s) and provide data origin authentication and integrity protection.

2. The responder sends: HDR, T, [IDr], V

   Timestamp payload (T) is used to provide anti-replay protection, ID payload is used to identify peer and verification payload (V) provides data origin authentication and integrity protection.

A new MBMS delivery exchange is defined. It contains the following messages:

1. **The BM-SC sends: HDR, IDi, MBMSKEY**

   ID payload is used to identify peer and MBMS key data transport payload (MBMSKEY) provides keys, anti-replay protection of keys and data origin authentication and integrity protection.

2. **The UE sends: HDR, IDr, V**

   ID payload is used to identify peer and verification payload (V) provides anti-replay protection, data origin authentication and integrity protection.

The idea is to minimize number of used payloads so that bandwidth is conserved. The timestamp payload provides anti-replay protection in the basic MIKEY. The

objective is to detect expired keys, not replayed messages. The desired functionality can be provided using version numbers in keys. If an attacker modifies the key bundle version field in the MBMSKEY payload then MAC verification fails. The MAC calculation of verification payload includes the original request message and IDr, so the BM-SC can detect if same response message is sent multiple times. Security policy can be defined in the service announcement so it is not required during the key delivery. Data origin authentication and integrity protection are provided using the MAC field of the MBMSKEY payload in initiator's message and the verification payload in the responder's message.

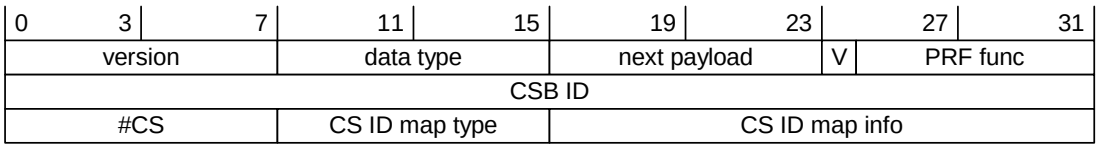
5 TEK Delivery

TEK delivery utilizes the same message flow as BAK delivery above, but the response message is omitted.

6 MIKEY Payloads

6.1 Header

The MIKEY header format is the following:



The common header contains the following information:

- version: the version number of MIKEY.

  version = 1

  No modifications. This is not changed, because existing exchanges or payloads are not changed.

- data type: describes the type of message (e.g. public-key transport message, verification message, error message).

Data type	Value	Comment
Pre-shared	0	Initiator's pre-shared key message
PSK ver msg	1	Verification message of a Pre-shared key message
Public key	2	Initiator's public-key transport message

		transport message
PK ver msg	3	Verification message of a public-key message
D-H init	4	Initiator's DH exchange message
D-H resp	5	Responder's DH exchange message
Error	6	Error message

The following types should be added:

Data type:	**Value:**	**Comment:**
MBMS upd req	**7**	**BM-SC's MBMS key update request message**
MBMS upd resp	**8**	**UE's MBMS key update response message**

Basic MIKEY implementation can ignore the message, when data field contains MBMS update message.

- next payload: identifies the payload that is added after this payload. **New type is added:**

Next Payload:	**Value:**	**Comment:**
MBMSKEY	**13**	**MBMS key data transport payload**

- V: flag to indicate whether a verification message is expected or not (this has only meaning when it is set by the Initiator). **No modifications.**

  V = 0 ==> no response expected **(used in TEK update request)**

  V = 1 ==> response expected **(used in BAK update request)**

- PRF func: Indicates the PRF function that has been/will be used for key derivation etc.

PRF func	Value	Comments
MIKEY-1	0	Mandatory, Default (see Section 4.1.2-3)
MIKEY-256	1	as MIKEY-1 but using a HMAC with SHA256
MIKEY-384	2	as MIKEY-1 but using a HMAC with SHA384
MIKEY-512	3	as MIKEY-1 but using a HMAC with SHA512

Not used in the Combined method. Set to 4 (0 is already used)

The following value should be added:

PRF func	**Value**	**Comments**
NULL	**4**	**PRF is not used**

- CSB ID: A 32-bit integer to identify the CSB. It is RECOMMENDED that it is chosen at random by the Initiator. This ID MUST be unique between each Initiator-Responder pair, i.e., not globally unique. An Initiator MUST check for collisions when choosing the ID (if the Initiator already has one or more established CSB with the Responder). The Responder uses the same CSB ID in the response.

  CSB ID and IDi shall uniquely identify the service.

- #CS: Indicates the number of Crypto Sessions that will be handled. Note that even though it is possible to use 255 CSs, it is not likely that a CSB will include this many CSs. The integer 0 is interpreted as no CS included. This may be the case in an initial setup message.

  Not used. Set to zero.

- CS ID map type: specifies the method to uniquely map Crypto Sessions to the security protocol sessions. SRTP-ID = 0.

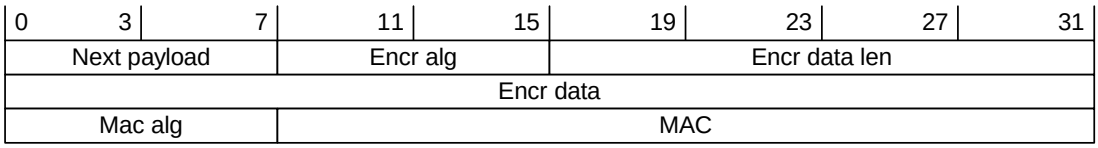
  Not used. Set to zero.

- CS ID map info: Identifies the crypto session(s) that the SA should be created for. The currently defined map type is the SRTP-ID

Not used. Set to zero.

6.2 MBMS Key Data Transport Payload (MBMSKEY)

The original key data transport payload has the following format:



The KEMAC contains the following information:

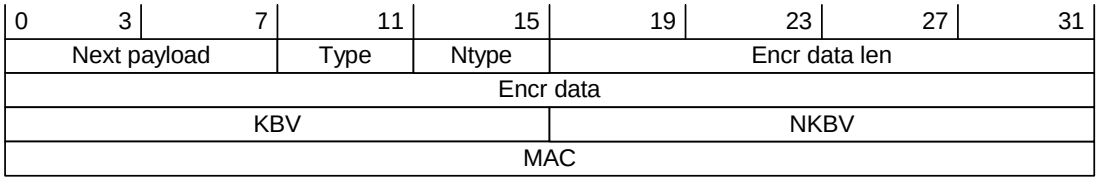
- Next payload: identifies the payload that is added after this payload.
- Encr alg: identifies the encryption algorithm used to encrypt the Encr data field
- Encr data len: length of Encr data
- Encr data: the encrypted key sub-payloads
- MAC alg: specifies the authentication algorithm used
- MAC: the message authentication code of the entire MIKEY message

A new MBMS key data transport payload (MBMSKEY) was defined, because the original key data transport payload (KEMAC) does not contain version numbers for keys. Version numbers are used, because:

- Anti-replay protection of keys can be provided without clock synchronization or reply cache
- MBMS security associations (keys) don't require lifetimes. The MBMS data messages and MBMS key delivery messages identify the current key
- Version numbers use less space than entire timestamp payloads

Encryption and MAC algorithm identifiers are removed, because the service announcement could contain this kind of static information. There is no reason to change the used algorithm during the MBMS service. CSB ID and IDi identify the current MBMS security association (used algorithms and key lengths). The MBMSKEY contains two version fields, one for the keys used to protect the Encr data field and one for the keys delivered inside the Encr data field. There are no separate version fields for MAC and encryption keys, because they can be changed at the same time. Type fields are added so that MBMS key exchange can be used to deliver BAKs and TEKs. It should be noted that it is possible to use KEK to protect both TEK and BAK. This can be useful feature if keys are wanted to deliver before the actual start of broadcast. The carried keys are identified (Ntype, NKBV) at the MBMS key level, because the receiver can skip decryption of Encr data field and

checking of MAC if it has already the current keys. The MBMSKEY format is the following:



The MBMSKEY contains the following information:

- **Next payload: identifies the payload that is added after this payload, see 6.1.**

- **Type: identifies the key level used to protect the Encr data field**

Type:	**Value:**	**Comment:**
KEK	**0**	**KEK level keys are used to protect MBMS key data delivery**
BAK	**1**	**BAK level keys are used to protect MBMS key data delivery**
RESERVED	**2-255**	

- **Ntype: Identifies type of keys, which are delivered inside the Encr data field**

RESERVED	**0**	
BAK	**1**	**BAK level keys**
TEK	**2**	**TEK level keys**
RESERVED	**3-255**	

- **Encr data len: Length of encrypted part (in bytes)**

- **Encr data: The encrypted key sub-payloads. It contains one or two sub-payloads. If the MAC is not used then it contains only sub-payload for the encryption key.**

- **KBV: Key bundle version, which is used to protect MBMS key delivery.**

- **NKBV: New key bundle version, which is used to identify keys inside the Encr data field**

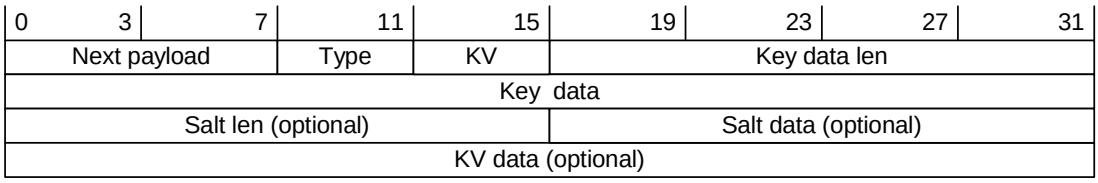
- **MAC: the message authentication code of the entire MIKEY message**

The following table summarizes information, which is required to map algorithms and keys:

Required information in UE:	Mapped entity:
CSB ID, IDi	MBMS security policy (used encryption and MAC algorithms)
CSB ID, IDi, Type, KBV	The current keys used to protect Encr data field
CSB ID, IDi, Ntype, NKBV	The delivered keys inside the Encr data field

6.3 Key Data Sub Field

The original key data sub field is used to transport actual keys. Key data sub field has the following format:



The key data sub field contains the following information:

- Next payload: identifies the payload that is added after this payload. **See 6.1.**

- Type: Indicates the type of the key included in the payload. 0-3 are used by the basic MIKEY. **New types should be defined. 4 for MBMS encryption key and 5 for MBMS MAC key.** The MBMSKEY payload identifies key level (BAK/TEK) so sub payload only need to indicate purpose of key (encryption or MAC).

- KV: Indicates the type of the key validity period. **No modifications. Set to zero.**

- Key data len: The length of Key data field. **No modifications.**

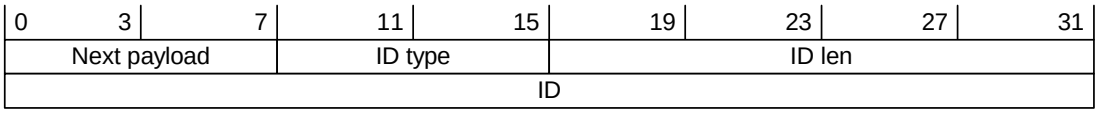
- Key data. **No modifications.**

- Salt len: The salt key lenght in bytes. **Not used.**

- Salt data: The salt key data. **Not used.**
- KV data. used to specify key validity period. **Not used.**

6.4 ID Payload

The identity payload has the following format:

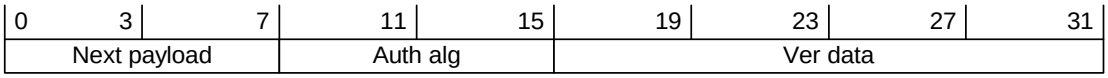


The identity payload has the following information:

- Next payload: identifies the payload that is added after this payload. **See 6.1.**
- ID type: specifies the identifier type used. The following types are supported: Network Access Identifier (NAI) and Uniform Resource Identifier (URI). **No modifications.**
- ID len: the length of the ID.
- ID: The ID data.

6.5 Verification Payload

The verification payload uses the following format:



The verification payload has the following information:

- Next payload: identifies the payload that is added after this payload. **See 6.1.**
- Auth alg: specifies the MAC algorithm used for the verification message. **Security policy (including authentication algorithm) is specified during the service announcement, thus new values is required:**

Authentication algorithm:	**Value:**
Algorithm specified by external policy	**2**

- Ver data: the verification message data. **No modifications.**

MAC is calculated over the request message and IDr (HDR | IDi | MBMSKEY | IDr).

6.6 Summary of Changes

The MIKEY provides a general extension payload to extensions to MIKEY, but it was not used, because it provides method to define a new payload into existing exchanges. Enhancements required a new exchange type to minimize bandwidth usage and simplify key management and anti-replay protection. There was not any reason to use the general extension payload in new exchange. It was more reasonable to define the MBMSKEY payload, which was optimized for the MBMS.

Required additions to MIKEY are:

- New exchange using old payloads and one new payload
- New payload (MBMSKEY)
- New type definitions in some payloads

7 Processing of BAK/TEK Delivery Message

This chapter presents the processing of BAK or TEK delivery message. MIKEY uses separate unicast message for TEK delivery, multicast messages for BAK delivery or BAK delivery message can be included into the MBMS data messages. The actual delivery mechanism is transparent to the MIKEY processing. The UE uses the following procedure, when it receives a new BAK/TEK delivery message:

1. The UE receives delivery message.
2. The UE checks version of the MIKEY. If the version is not supported then MIKEY packet is discarded.
3. The UE checks data type in header. If the exchange (data type) is not supported then MIKEY packet is discarded.
4. The UE checks V field.

After the checking of data type and V fields, the UE knows that the current MIKEY message is a BAK or TEK delivery message.

5. The UE looks up MBMS security association using the CSB ID and IDi.
6. The UE checks NKBV and Ntype in MBMSKEY.

If the UE has not the current key or the BM-SC is delivering a new key beforehand (version number of carried key is bigger than the current version) then the UE continues processing of the key delivery message.

7. The UE checks that it has the current KEK or BAK level keys (Type and KBV fields in MBMSKEY).

8. The UE calculates MAC using the correct algorithm and key (algorithm is identified by MBMS security association and key is identified by Type and KBV). If MAC calculation fails then the MIKEY message is discarded.

9. The UE decrypts the Encr data field (algorithm is identified by MBMS security association and key is identified by Type and KBV) and retrieves keys. If the UE has not the current keys then old keys are replaced. Otherwise new keys are cached and taken into use, when the current keys are changed by the BM-SC.

8 Standardization Status

MIKEY has been approved by IESG and it has received the "Proposed Standard" status, thus presented enhancements cannot incorporate into basic MIKEY protocol. However, it is possible to create a new Internet-Draft and publish it later as an "Informational RFC".

9 Conclusions

This paper has presented efficient enhancements to MIKEY protocol so that it can be used to deliver encrypted keys to UEs. The design objectives of enhancements and every required extension are presented in detail.

Nokia proposes that the enhanced MIKEY is chosen as a key delivery protocol in SA3.

Nokia proposes that the following actions are taken to standardize enhancements:

1. IETF MSEC working group is contacted and informed about the enhancements.

2. A new "MIKEY MBMS extensions" Internet-Draft is published via IETF MSEC working group.

3. MIKEY MBMS extensions are published as an Informational RFC. If it impossible to publish RFC in time then required enhancements are incorporated into relevant 3GPP specifications.

10 References

[S3-030751] Further updates on Combined model for MBMS security, SA3#31 Novermber

[MIKEY] MIKEY: Multimedia Internet KEYing, draft-ietf-msec-mikey-08.txt