3GPP TSG SA WG3 Security — SA3#36 **S3-041017**

November 23 - 26, 2004

Shenzen, China

Title: **Key group ID and MSK ID**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

This contribution studies if Key group ID can be merged to MSK ID and how the key IDs are carried in MSK and MTK messages.

2 Discussion

2.1 Combining Key group ID and MSK ID

Current TS 33.246 [1] identifies MSK keys as follows 6.3.2.1:

Every MSK is uniquely identifiable by its Network ID, Key Group ID and MSK ID

where

Network ID = MCC || MNC and is 3 bytes long. It is carried in the IDi payload in MIKEY message

Key Group ID is 2 bytes long and is used to group keys together in order to allow redundant MSKs to be deleted. It is carried in the CSB ID field of MIKEY common header.

MSK ID is 2 bytes long and is used to distinguish MSKs that have the same Network ID and Key Group ID. It is carried in the MSK-ID field of MIKEY extension payload.

There are some reasons why Key Group ID should be merged to MSK ID.

1. The Key Group ID is always related to MSK ID. There seems to be no functional reason why these should be carried separately.

2. Carrying Key Group ID and MSK ID together clarifies the usage of keys in MBMS. The relation between Key Group ID and MSK ID becomes evident.

3. Carrying Key Group ID in the CSB field of MIKEY is not semantically correct according to RFC 3830 since the CSB-ID field should identify the key material that was used to protect the MIKEY

message, i.e. the “outer key ID” in MBMS terms. Currently in MTK messages CSB ID carries only part of that information and in MSK messages it carries part of “inner key ID”.

4. MIKEY verification message includes also CSB ID field. Carrying Key Group ID in MSK verification message CSB ID field is unnecessary since it does not help identify the key, i.e. MUK, that was used to protect the verification message. This hints that MUK ID should be carried in CSB ID field of MSK messages, if possible.

5. The 2 byte Key Group ID is carried in 4 byte CSB ID field. This means that two bytes of are unused (i.e. wasted) in each MIKEY message. If Key Group ID is combined to MSK ID the result will be 4 bytes ID that will fit to CSB ID.

Therefore it is proposed to merge Key Group ID with MSK ID. The new ID could be a 4 byte concatenation Key Group ID with MSK ID. The meaning of the fields would be the same earlier. It is proposed to define the *new MSK ID* as follows:

MSK ID = (Service ID part || Key ID part) where

Service ID part is 2 bytes long and is used to group keys together in order to allow redundant MSKs to be deleted.

Key ID part is 2 bytes long and is used to distinguish MSKs that have the same Network ID and Service ID.

2.2 Carrying MTK ID and new MSK ID in MTK messages

It is proposed that the key IDs are carried in MTK message as follows:

- The new MSK ID (4 bytes) is carried in the CSB field of the common header. This identifies the “outer key” in MTK message.

- The MTK ID (2 bytes) is carried in the extension payload. This identifies the “inner key” in MTK message. Carrying only one key ID is possible according to the internet draft on MBMS extensions to MIKEY RFC, see another contribution from Ericsson.

This follows the semantics of RFC 3830 and saves 2 bytes for each MTK message since the new MSK ID fits exactly to CSB ID field.

2.3 Carrying MUK ID and new MSK ID in MSK messages

The MUK ID has not been defined yet, thus there are different alternatives how to carry the MUK ID and the new MSK ID in the MSK message. It should be noted that also the verification message needs to be taken into account.

1. The most natural way is to carry the MUK ID in the CSB ID field and MSK ID in the extension header, i.e. **the MSK message** looks like:

- The MUK ID is carried in the CSB field of the common header. This identifies the “outer key” in MSK message.

- The MSK ID (4 bytes) is carried in the extension payload. This identifies the “inner key” in MSK message. Carrying only one key ID is possible according to the internet draft on MBMS extensions to MIKEY RFC, see another contribution from Ericsson.

The **MSK verification message looks** like:

- The MUK ID is carried in the CSB field of the common header. This identifies the “outer key” in MSK verification message.

- The MSK ID (4 bytes) does not need to be carried in the verification message.

This alternative requires that MUK ID fits into the CSB ID field. A proposal for MUK ID is presented in another Ericsson contribution.

2. If the MUK ID does not fit into the CSB ID field, it is possible to carry both MUK ID and MSK ID in the new extension payload, i.e. **the MSK message** looks like:

- The MUK ID is carried in the extension payload. This identifies the “outer key” in MSK message.

- The MSK ID (4 bytes) is carried in the extension payload. This identifies the “inner key” in MSK message. Carrying also two key IDs is possible according to the internet draft on MBMS extensions to MIKEY RFC, see another contribution from Ericsson.

The **MSK verification message looks** like:

- The MUK ID is carried in the extension payload. This identifies the “outer key” in MSK message.

- The MSK ID (4 bytes) does not need to be carried in the verification message.

This alternative has the drawback that it leaves CSB ID field empty in both directions and the use of CSB ID field is against the semantics of RFC 3830.

3. If the MUK ID does not fit into the CSB ID field and in order to use the CSB ID field, it is possible to carry MUK ID in the new extension payload and MSK ID in the CSB field. The use of CSB ID field is against the semantics of RFC 3830 but it would save 4 bytes, i.e. **the MSK message** looks like:

- The MSK ID (4 bytes) is carried in the CSB field of the common header. This identifies the “inner key” in MSK message. This identifies the “inner key” in MSK message. Carrying also two key IDs is possible according to the internet draft on MBMS extensions to MIKEY RFC, see another contribution from Ericsson.

- The MUK ID is carried in the extension payload. This identifies the “outer key” in MSK message.

The **MSK verification message looks** like:

- The MSK ID (4 bytes) does not need to be carried in the verification message, but the CSB ID field can carry it.

- The MUK ID is carried in the extension payload. This identifies the “outer key” in MSK verification message.

This alternative has the drawback that it leaves CSB ID field empty in the MSK verification message and the use of CSB ID field is against the semantics of RFC 3830.

3 Conclusions and proposal

In order to clarify the usage of key identities and to align with RFC 3830, this contribution has proposed to combine Key Group ID and MSK ID into a new MSK ID that would be MSK ID = (Service ID part || Key ID part).

This contribution analysed how to carry MUK ID, new MSK ID and MTK ID in MIKEY messages.

- It is proposed that alternative 1 is chosen for the **MSK message**. I.e. MSK message carries MUK ID in CSB ID field and new MSK ID in extension payload. This is according to semantics of CSB field in RFC 3830 and it does not send empty fields. This proposal depends on the decision on MUK ID, see contribution. If MUK ID is too long to be carried in the CSB ID field, it is proposed to choose alternative 3.

- It is also proposed that MTK message carries new MSK ID in CSB ID field and new MSK ID in extension payload.

A CR from Ericsson to this meeting proposes needed changes in TS 33.246.

4 References

[1] TS 33.246, Security of MBMS