**3GPP TSG SA WG3 Security — S3#37** **S3-050099**
**21 – 25 February 2005** **(same as cover for S3-050083)**
**Sophia Antipolis, France**

**Source:** **Ericsson**

**Title:** **More reliable acknowledgement of MSK delivery**

**Document for:** **Discussion and decision**

**Agenda Item:** **MBMS**

# 1 Introduction

In some cases, e.g., when the charging is to be based on MSK delivery, it is crucial to be able to rely on that the UE has received the MSK to provide a robust charging scheme. It is not good enough to rely on the UE to send an acknowledgement of the reception, since a malicious UE could refrain from sending such a message. The following is a proposal to increase the reliability of the acknowledgement.

# 2 A proposed solution

To increase the chance that the UE stays honest and delivers the acknowledgement to the BM-SC the approach described below could be taken. Note that it is assumed that MGV-F and MGV-S resides in a secure place in the UE.

1. The UE receives the MSK message and delivers it to the MGV-F. The MGV-F unpacks the MSK, stores it in the MGV-S and marks it as inactive.
2. The UE sends an MSK acknowledgement message back to the BM-SC in the MIKEY verification message.
3. Upon reception of the acknowledgement, the BM-SC sends an “activation-message” back to the UE (could be done by another MIKEY verification message).
4. The UE receives the activation message and hands it over to the MGV-F. The MGV-F marks the MSK as active.
5. The UE sends an acknowledgement message back to the BM-SC.
6. If the BM-SC does not receive the acknowledgement to the activation message within a predetermined time, the BM-SC resends the activation message.

The MGV-F does not give the UE any keys protected by the MSK until it is marked as active.

# 3 Analysis of the proposed solution

The above solution is not waterproof, but it ensures that malicious users are forced to pay, and it increases the probability that honest users are fairly charged.

A malicious user that refuses to send the MSK reception acknowledgement message back to the BM-SC will not be able to use the MSK since it will be marked as inactive, and will hence be denied service.

A honest user may receive the MSK delivery, send the reception acknowledgement and get charged, but then the MSK activation message from the BM-SC to the UE may be lost. In this case the user will be charged for a service he will not be able to use. To increase the probability that the message arrives at the UE, steps 5 and 6 are added above. Note that a the UE has already been charged for the MSK, so there is no point for a malicious ME to not send the acknowledge of the activation message.

It should be noted though that the all three messages (MSK delivery, reception acknowledgement and MSK activation message) are sent in sequence, and if the first two messages are correctly delivered, it is also likely that the third message (the activation) will be delivered correctly. Typically, if the UE is in radio coverage with lousy radio-conditions all messages gets through on the interactive bearer (albeit at a lower bit-rate). If the UE is out of radio coverage, all messages are lost and the UE will not be charged.

# 4 Conclusion and proposal

The proposed solution gives a more robust way of charging users based on MSK reception than the current two-way “handshake”. It is proposed that the accompanying CR [2] is implemented in TS 33.246 [1].

# 5 References

[1] TS 33.246, “Security of MBMS service”, 3GPP
[2] S3-050xxx, “More reliable MSK delivery”, SA3#37, Ericsson

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

***Tdoc ⌘Att_S3-050099***

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **33.246** **CR** **046** ⌘ **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:*** | ⌘ | More reliable MSK delivery based charging |
| ***Source:*** | ⌘ | Ericsson |
| ***Work item code:*** | ⌘ | MBMS |
| ***Date:*** | ⌘ | 2005-02-14 |
| ***Category:*** | ⌘ | **B** |
| ***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:*** | ⌘ | Some services based on MBMS will charge according to delivered MSKs. The CR implements a proposal that increases the reliability of the MSK delivery. It stops dishonest users from denying getting the key, and increases the probability that honest users receive the key they are charged for. |
| ***Summary of change:*** | ⌘ | • An extended MSK exchange procedure is introduced to prevent that malicious UE does not acknowledge the MSK. Under the assumption that if two messages gets through the channel, it is more likely that a third one also will.<br>• A clarification of the contents of the CSB ID field is made. Currently the text can be interpreted so that the CSB ID field is not present.<br><br>The CR partially overlaps with Samsung CR S3-050088. |
| ***Consequences if not approved:*** | ⌘ | Charging based on MSK delivery will be less reliable. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 6.3.2.3.3, 6.4.2, 6.5.3, 6.5.4 |

| ***Other specs Affected:*** | Y | N | | |
|---|---|---|---|---|
| ⌘ | Y | | Other core specifications | ⌘ TS 31.102 |
| | | N | Test specifications | |
| | | N | O&M Specifications | |

***Other comments:*** ⌘

#### 6.3.2.3.3 MSK acknowledgement reliability procedure

To increase the reliability of MSK delivery (typically to improve robustness of charging) the following procedure can be used where the BM-SC sends an activation message for an MSK, which has to be received and verified by the MGV-F before the MSK can be used by the UE.

NOTE: The procedure can be used in situations where the charging is based on delivered MSKs. The procedure avoids that a malicious UE refrains from sending the MIKEY ACK in order to avoid getting charged for the MSK.

The first message constitutes an MSK delivery message as in the regular case, but the Key Validity data of the MSK is such that the lower limit SEQs is greater than the upper limit SEQu according to RFC 1982 [10]. This implies that the MSK is not valid for use with any MTK, i.e., it is 'inactive'.

The MSK delivery message is acknowledged by the UE. When the BM-SC receives the MIKEY ACK, it can generate a charging record for the subscriber. Next the BM-SC sends a new MSK delivery message to activate the MSK in the UE; this time the Key Validity data of the key is the one desired by the BM-SC (i.e., SEQs is smaller than SEQu).

When the UE has received the second MSK delivery message (and has handed it over to the MGV-F), it is able to use the MSK, and sends a MIKEY ACK for the MSK message to the BM-SC.

This instantiates a four-way procedure instead of the regular request-response procedure. The processing of the activation message is described in clause 6.5.3. The four-way procedure is shown in Figure 6.3a.

If the UE tries to use an 'inactive' MSK, the MGV-F will respond with an error and the UE may request the MSK again from the BM-SC. This will trigger a new MSK delivery procedure.

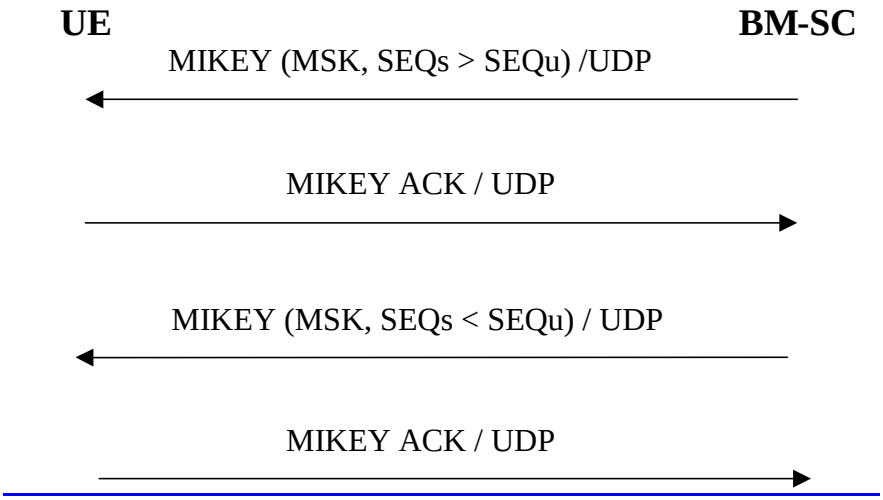


**Figure 6.3a: Pushing the inactive MSKs to the UE, followed by the activation.**

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

### 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 shall be set to all zeros~~is not used~~.

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

## 6.5.3 MSK processing

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the EXT. If the key in the message is an MSK protected by MUK, MGV-F retrieves the MUK identified as specified in clause 6.1.

The integrity of the message is validated and the MSK is extracted from the KEMAC payload as described in section 5 of reference [9] if the validation is successful. The Key Validity data is extracted from the message and stored (in the form of MTK ID interval). The lower limit of the interval defines the SEQs and the upper limit defines the SEQu.

NOTE: The MSK is not necessarily updated in the message, since a MSK transport message can be sent e.g. to update the Key Validity data.

If message validation is successful, then the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MUK ID.

## 6.5.4 MTK processing

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the EXT. If the key inside the message is an MTK protected by MSK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence numbers SEQs and SEQu, have been stored within a secure storage (MGV-S). ~~Both~~ MSK, ~~and~~ SEQs and SEQu were transferred to the MGV-S with the execution of the MSK update procedures. The initial values of SEQs and SEQu ~~is~~ are determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs and SEQu according to RFC 1982 [10]. If SEQp is equal or lower than SEQs or greater than SEQu, or if the SEQs is greater than SEQu, then the MGV-F shall indicate a failure to the ME. The MGV-F shall not process any messages that depend on an 'inactive' MSK (see clause 6.3.2.3.3). ~~If SEQp is greater than SEQs then~~ Otherwise the MGV-F shall verify the integrity of the MIKEY message according to RFC 3830 [9]. If the verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the verification is successful, then the MGV-F shall update SEQs with SEQp value and extract the MTK from the message. The MGV-F then provides the MTK to the ME.

If MAC verification is successful, the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

In the case of streaming, SRTP requires a master key and a master salt. The MTK is used as master key, and the salt in the KEMAC payload is used as master salt.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of RFC 3830 [9] (MIKEY).

In case of download service, MIKEY key derivation as defined in section 4.1.3 of MIKEY [9] shall be used to derive MTK authentication and encryption keys from MTK in the ME. These keys shall be provided to the download protection protocol.