3GPP TSG SA WG3 Security — S3#37 S3-050072

21 - 25 February 2005

Sophia Antipolis, France

Source: Siemens

Title: MSK verification message handling

Agenda item: MBMS

Document for: Discussion/Decision

1 Introduction

If the BM-SC requires an MSK verification message, then after calling the ‘MSK update Procedure’ (Figure D.1), the ME will have to call a separate procedure ‘MSK Verification Message Generation’ (Figure D.2). In order to prevent a malicious ME to sign an arbitrary MSK verification message, the following measure was specified in Annex D.2 [1] : “ *The UICC will verify that the Time Stamp MIKEY field corresponds to the previous MSK Update procedure*”. It will be shown in this contribution that the realization of ‘previous’ is unclear. It will also be shown that the current realization (i.e. two-step MSK verification message generation) introduces some restrictions on the ME handling. Also some security considerations are given on the way this two-step MSK verification generation function is specified.

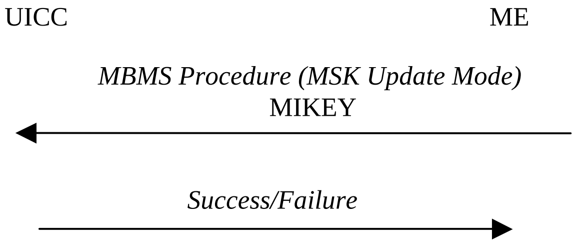


Figure D.1: MSK Update Procedure

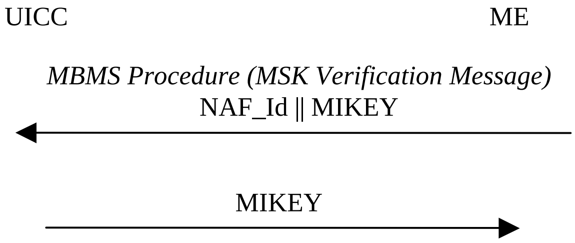


Figure D.2: MSK Verification Message Generation

2 Discussion

The only verification check that (according to [1] Annex D.2) need to be done is to check if the TS (TimeStamp) field from the input verification message, corresponds to the previous MSK update message. This TimeStamp check measure was introduced to avoid that a malicious ME could let the MGV-F sign arbitrary messages. From the specification it is not clear whether this ‘previous’ TimeStamp is to be maintained per MUK (i.e. NAF-ID/B-TID combination) or per UICC (i.e. one value). A per UICC counter is not an option as it would allow for misusing the TS correlation mechanism to let the UICC sign an arbitrary message and thereafter could allow for re-sending the signed message to the UICC as a MSK update message, resulting in a UICC MBMS DoS attack. The TS-check will not prevent the ME in submitting non-verification messages to the UICC. Whether the UICC would reject to sign MIKEY messages that syntactically do not correspond to MIKEY verification messages, depends on the implementation.

In further analysis we assume that Annex D.2 TS correlation would be clarified in the following way:

“The UICC uses the MUK ID (see clause 6.1) to identify the stored Ks_int_NAF=MUK to be used in the MSK Verification Message Generation. The UICC will verify that the Time Stamp MIKEY field correspond to the Time Stamp of the last accepted MSK UpdateProcedure of the related MUK-ID.~~previous MSK Update procedure~~. Then, the UICC shall compute and send the MIKEY packet to the ME (including the calculated MAC field) as defined in clause 6.4.5.2. (MSK Verification message).”

The aim of the above formulation should be that a MAC (and signed message) which is generated via the MSK verification message generation procedure for a certain MUK-ID can not be replayed towards the MSK update message procedure. This should not be the case while the TS of any received MSK update message of a particular MUK-ID shall be greater than the last accepted TS, and the verification message that is proposed to be signed by the ME, cannot include a TS greater than the last accepted one of the MSK update procedure of that particular MUK-ID.

The proposed interpretation (see *italic* text above) however makes it impossible for the ME to execute following parallelism scenario per NAF-ID:

1) Update MSK=5 message to UICC successfully (TS=7)
2) Update MSK=6 message to UICC successfully (TS=8)
3) Call MSK Verification Message Generation procedure (TS=7), rejected due to not matching time stamp.
4) Call MSK Verification Message Generation procedure (TS=8), accepted

A solution to allow the above scenario (and maintaining the current two-step procedure approach) is to require the UICC to remember the list of not yet handled TS which require a verification message. In that case the UICC will have to store more then one Time Stamp (i.e. in this case the UICC has to maintain some state).

Another simple solution is to disallow the parallel execution within the ME. In this case, a NOTE should be added to the specification to point to the restriction. Also an error message needs to be added in Figure D.2.

A third more impacting solution, is to redesign the interface for MSK generation and verification. The verification message generation could be handled in the same procedure as the MSK update, so removing the need for TS time stamp lists (or any other equivalent message correlation mechanisms). Such a procedure would look as follows:

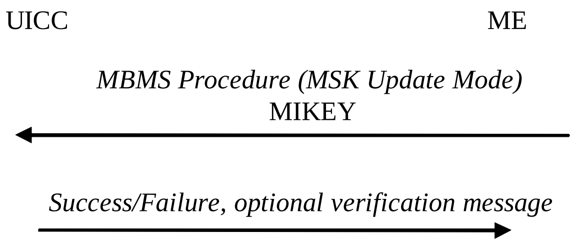

UICC
ME
MBMS Procedure (MSK Update Mode)
MIKEY
Success/Failure, optional verification message

Figure 2: New MSK Update Procedure

The advantages of this solution are:

A) The ME cannot try to misuse the MSK verification generation mechanism to generate needless verification messages.

B) No solution (or restriction) has to be sought for the parallelism scenario.

C) Simpler success/failure handling (avoid error situations e.g. ME giving a wrong NAF-ID, or other input parameters).

D) An ME (e.g. virus infected) cannot misuse the interface to generate MAC's on arbitrary (malformed) MIKEY (verification) messages. The potential threat on the misuse of the interface results from a lack of implementation recommendations for the check of the MIKEY message format.

3 Conclusion

Siemens prefers to implement option 3: 'redesign the interface for MSK generation and verification'. This approach has been implemented in the accompanying CR to TS 33.246. If this proposal is accepted, T3 needs to be informed of this change.

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

Tdoc ⌘Att_S3-050072

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.246**	**CR**	**037**	⌘ **rev**	**-**	⌘	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

Title:	⌘	Correct the MSK verification message handling		
Source:	⌘	Siemens		
Work item code:	⌘	MBMS	***Date:*** ⌘	14/02/2005
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:	⌘	The verification by the UICC that the inserted Time Stamp Field in the -to be signed-MIKEY packet shall match the previously handled MSK update procedure restricts the ME handling. It will cause an error if the ME would handle multiple MSK Update messages before generating the MSK verification messages. Furthermore the error handling in case the Time Stamp check would fail, is unspecified yet. From a security point of view, it has to be ensured that the ME cannot ask the UICC to sign arbitrary messages.
Summary of change:	⌘	Correct the description of MSK verification message handling for Time stamp handling. The two procedures ‘MSK Update’ and ‘MSK verification’ are combined into one procedure.
Consequences if not approved:	⌘	Parallel handling of MSK update message is not possible. More error situations for MSK updates/verification handling. A malicious ME may let the UICC sign (arbitrary) message when not needed.

Clauses affected:	⌘	6.4.5.2, Annex D.2				
		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 31.102
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

===== BEGIN CHANGE =====

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 || IDr || V, where 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 ID 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.

Common HDR
TS
IDr
V

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 verification message, when received as result from the MGV-F, ~~–~~to the BM-SC.

===== END CHANGE =====

Annex D (normative): UICC-ME interface

D.1 MSK Update Procedure

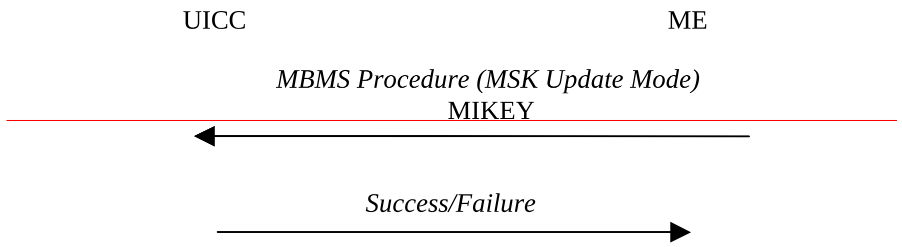
This procedure is part of the MSK update procedure as described in clause 6.5 (Validation and key derivation functions in MGV-F).

The ME has previously performed a GBA_U bootstrapping procedure as described in TS 33.220. The UICC stores the corresponding Ks_int_NAF together with the NAF_Id associated with this particular bootstrapping procedure.

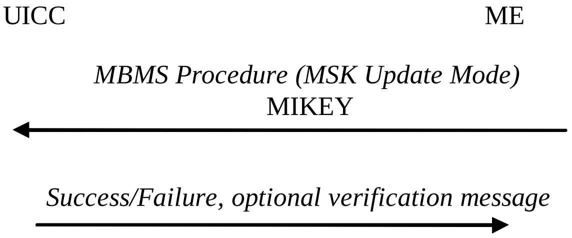
The ME receives a MIKEY message containing an MSK update~~ procedure~~. After performing some validity checks, the ME sends the whole message to the UICC. The UICC uses the MUK ID (included in the MIKEY message, see clause 6.1) to identify the stored Ks_int_NAF.

The UICC then uses Ks_int_NAF as the MUK value for MUK derivation and MSK validation and derivation (as described in clause 6.5.3).

After successful MSK Update procedure the UICC stores the Key Domain ID, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).



~~Figure D.1: MSK Update~~


UICC
ME
MBMS Procedure (MSK Update Mode)
MIKEY
Success/Failure, optional verification message

~~Procedure~~

Figure D.1: MSK Update Procedure

In case the MSK update MIKEY message is acceptable and the V-bit was set in the HDR, then a MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message) shall be produced. The UICC uses the same MUK ID and TS, which were received from the MSK MIKEY Message (see clause 6.1), for the MSK Verification Message Generation.

D.2 Void

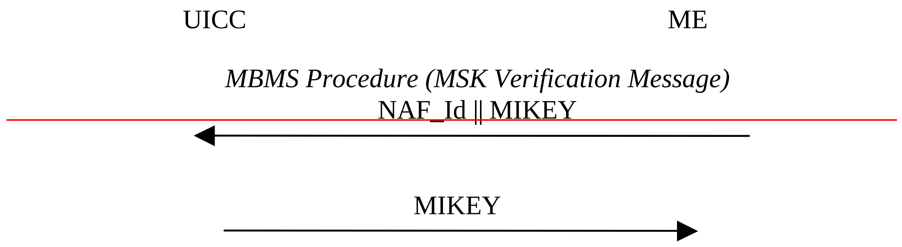
~~MSK Verification Message Generation~~

~~This procedure is part of the MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message).~~

~~The ME constructs the verification message in response to the MSK-transport message when it is required by BM-SC.~~

~~The ME shall then give the constructed MIKEY verification message, with an empty MAC field, to the UICC and the ME shall include NAF_id in this message. The UICC uses the MUK ID (see clause 6.1) to identify the stored Ks_int_NAF=MUK to be used in the MSK Verification Message Generation.~~

~~The UICC will verify that the Time Stamp MIKEY field correspond to the previous MSK Update procedure. Then, the UICC shall compute and send the MIKEY packet to the ME (including the calculated MAC field) as defined in clause 6.4.5.2. (MSK Verification message).~~



~~Figure D.2: MSK Verification Message~~

D.3 MTK generation and validation

This procedure is part of the MTK generation and validation function as described in clause 6.5.4 (MTK validation and derivation).

The ME receives the MIKEY message (containing Header, Time stamp, Key Domain ID, MSK ID, MTK ID = SEQp, MSK_C[MTK||Salt (if salt is available)] and MAC). After performing some validity checks, the ME sends the whole message to the UICC. The UICC computes the MGV-F function as described in clause 6.5. (Validation and key derivation functions in MGV-F). After successful MGV-F procedure the UICC returns the MTK.

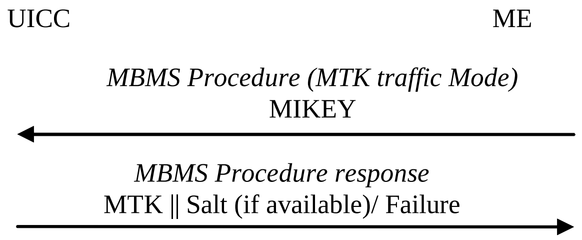

UICC
ME
MBMS Procedure (MTK traffic Mode)
MIKEY
MBMS Procedure response
MTK || Salt (if available)/ Failure

Figure D.3: MTK Generation and Validation

===== END CHANGE =====