3GPP TSG SA WG3 Security — SA3#36 **S3-040997**

November 23 - 26, 2004

Shenzhen, China

Title: **Replacing Network ID with NAF ID**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

Currently the MBMS Service key (MSK) is identified by Network ID, Key Group ID and MSK ID [1]. MTK is identified by the above plus MTK ID. The Network ID is defined as MCC/MNC. This contribution discusses some concerns on usage of MCC/MNC and studies if NAF ID could be used instead.

2 Concerns on MCC/MNC

The following concerns have been identified for using MCC|MNC in MBMS.

Concern 1: Consider the following example. A Swiss operator may send MBMS data originating from operators in France or Italy (i.e. the BM-SC is not in the same network as the UE). If the originator sets the Network ID, the MCC/MNC is then not "what one expect" in the Swiss network on the radio level, which would have different MCC/MNC value.

Concern 2: Consider another example. An operator having might use MBMS over WiFi or other non-3GPP technology in the future. How should the operator populate MCC/MNC?

Concern 3: The MCC/MNC is operator specific parameter. Keeping in mind the MBMS key identification chain it should be ensured that BM-SCs within one operator (MCC/MNC) shall not share Key Group IDs.

Possible solution to concern 1 could be a note in the specifications that the UE should not try to interpret the MCC/MNC nor compare it to the MCC/MNC of the current network where the UE is connected.

Possible solution to concern 2could be that an operator using non-3GPP system could reserve a MCC/MNC value from ITU to ensure that the used MCC/MNC is globally unique.

Possible solution to concern 3 could be a note in the TS to specify that it should be ensured that Key Group IDs are unique between BM-SCs.

Another solution would be to use NAF ID instead of MCC/MNC.

3 Using NAF ID in MBMS

3.1 NAF ID solves concerns

Using NAF-ID could solve the concerns presented above:

- Concern1: NAF ID is not associated to any radio level identifiers
- Concern2: NAF ID is not 3GPP specific identifier
- Concern3: NAF ID uniquely identifies each BM-SC

3.2 Analysis

If NAF ID (FQDN) as specied in GBA should replace MCC/MNC, the following needs to be taken into account.

3.2.1 NAF ID within Key management

The MSK (and MTK) would be identified with NAF ID, Key group ID, MSK ID (plus MTK ID for MTK). This would give BM-SC specific key identifiers.

In key management, NAF ID would be carried in IDi field of MIKEY [2] messages (both MSK and MTK messages). NAF ID can be considerably longer, than MCC/MNC, which is 3 bytes. Therefore the overhead could become a problem in MSK and MTK messages.

In case of sending MSKs, the overhead may not be a problem in MSK messages, since they are sent quite rarely.

In case of sending MTK messages with the download traffic the overhead may not be a problem, since the MTK message is not sent frequently, but it is incorporated as a download object into FLUTE.

However, the overhead may become a problem in MTK messages if they are sent frequently. For example in streaming case the MTK messages could be sent even every few seconds in some scenarios. Two alternatives to overcome this are foreseen:

1. The NAF ID would *not* be sent in MTK messages (it is optional parameter in MIKEY). Instead, the source IP address could be mapped to the NAF ID. Internally in the UE, the ME could send the NAF ID and MTK message separately to the MGV-F (UICC). The same solution should be applied to MTK messages in download also since the ME-UICC interface should be similar for streaming and download services.

2. The NAF ID could be sent in a compressed form in order to cut down the overhead. The exact way of compressing is FFS and could be stage-3 work.

Alternative 1 is not recommended since it ties the MBMS security to IP layer.

3.2.2 NAF ID within traffic

Network ID is currently sent in MKI (Master Key Identifier) field, which is carried in every SRTP packet. NAF ID would increase the overhead of MKI considerably. However, as it is shown is another contribution [3], Network ID (or NAF ID) is not actually needed in MKI field.

NAF ID would need to be sent also within download content to identify used protection keys. The overhead may not be a problem in this case, since there seems to be no need to repeat the key identifier information.

3.2.3 NAF ID usage in ME – UICC interface

TS 33.246 [1] Annex D.1 specifies that ME gives NAF ID and MIKEY message to the UICC in case of MSK update message. It is unclear how the ME receives the NAF ID in the first place. (It should be noted that if the MIKEY message includes the NAF ID there would be no need to send it separately.)

From Annex D.1 of TS 33.246:

> *… 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 ME also includes in this request NAF_Id to identify the stored Ks_int_NAF. …*

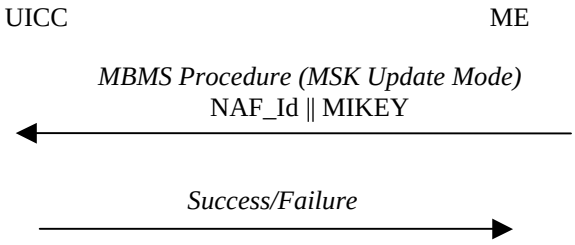

Figure D.1: MSK Update Procedure

4 Conclusions and proposal

This contribution has described some concerns related to the usage of MCC/MNC in MBMS security. The usage of NAF ID was analysed. NAF ID seems to address the raised concerns, but the overhead introduced by it may be a problem when MTKs are sent frequently in streaming services. According to Annex D of TS 33.246 it seems that NAF ID is needed also in ME-UICC interface to help identify the correct GBA key, i.e. MUK.

Two ways forward are seen:

1. Network ID is replaced with NAF ID. Functionally this should be feasible. However, then it needs to be decided if the length of NAF ID is a problem, especially in MTK messages in streaming case. If yes, a solution to deduce the NAF ID from elsewhere than MTK messages is needed (e.g. from destination or source IP address). For consistent handling on ME-UICC interface, similar solution should be developed also for download services. This choice may have also impact to format of MUK ID, see contribution on MUK –ID [4]).

2. Network ID is not replaced. In this case the presented concerns should be covered. In addition to this it should be ensured that the NAF ID is received by other means for MUK retrieval in UICC or that such solution should be made for MUK ID that NAF ID is not needed (see contribution on MUK ID [4]).

It is proposed that SA3 makes a decision which approach to adopt. A CR from Ericsson to this meeting proposes needed these two alternatives in TS 33.246. One of the alternatives should be chosen.

(It should be noted that these decisions may mean impacts to stage 3 terminal specifications, e.g. in TS 31.102, but this TS seems to require updates anyway since it does not currently use MUK ID in identifying the MUK. TS 31.102 has already taken the assumption that NAF ID will be used to identify MUK. See also contribution [4]).

5 References

[1] TS 33.246, Security of MBMS

[2] IETF RFC 3830, MIKEY: Multimedia Internet Keying

[3] TD S3-040xxx, Shorter MKI, Ericsson, SA3#36

[4] TD S3-040xxx, MUK ID and UE ID, Ericsson, SA3#36

3GPP TSG-SA3 Meeting #36
Shenzhen, China, 23 – 26 November

Tdoc ⌘Att1_S3-040997

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **025** ⌘ **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:	⌘	NAF ID in MBMS
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	12/11/2004
Category:	⌘	**C**
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:
2 (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)

Reason for change:	⌘	The network ID (MCC||MNC) is currently carried in IDi field of MIKEY messages. It has some drawbacks in MBMS security. The usage of NAF ID (full domain name of BM-SC) is an alternative, but it has also its own drawbacks. This CR introduces alternatives which propose the usage of MCC||MNC or NAF ID in MIKEY messages.
Summary of change:	⌘	The CR includes two alternatives a) MCC||MNC is used in IDi. b) NAF ID is used in IDi. Only one of the alternatives should be chosen and the CR should be revised accordingly.
Consequences if not approved:	⌘	Usage of IDi field remains unspecified.

Clauses affected:	⌘	Alternative A: 6.3.2.1, 6.4.5.1. Alternative B: 6.3.2.1, 6.3.3, 6.4.5.1, 6.4.6.2, 6.5.4, D.1, D.3

Other specs affected:	⌘	Y	N		⌘
		X		Other core specifications	TS 31.102
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	Two alternatives and their corresponding changes are presented in this CR

*********Alternative A: CR if network ID is not changed***begin******

6.3.2.1 MSK identification

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.

NOTE: When MCC || MNC is used as key identifier, the UE shall not try to use it in another context. E.g. UE should not compare the received MCC || MNC to parameters in radio level.

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.

NOTE: It shall be ensured that the Key group IDs are unique within an operator, i.e. two BM-SCs within an operator shall not use the same Key Group ID value.

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.

If the UE receives an MSK and already contains two other MSKs under the same Network ID and Key Group ID, then the UE shall delete the older of these two MSKs.

Editor's Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.

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

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~~ includes the MCC||MNC. 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.

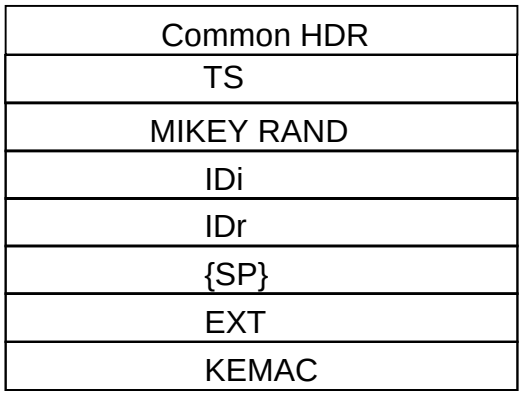

Figure 6.5: The logical structure of the MIKEY message used to deliver MSK. For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

********* Alternative A: CR if network ID is not changed***end******

********* Alternative B: CR if network ID is changed***begin******

6.3.2 MSK procedures

6.3.2.1 MSK identification

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

where

~~Network ID = MCC || MNC and is 3 bytes long.~~ NAF ID is as defined in TS 33.220 [6]. 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~~ NAF ID and Key Group ID. It is carried in the MSK-ID field of MIKEY extension payload.

If the UE receives an MSK and already contains two other MSKs under the same ~~Network~~ NAF ID and Key Group ID, then the UE shall delete the older of these two MSKs.

Editor's Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.

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

6.3.3 MTK procedures

6.3.3.1 MTK identification

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

where

~~Network~~ NAF ID, Key Group ID and MSK ID are as defined in clause 6.3.2.1.

Editor's Note: The format of MTK is ffs.

6.3.3.2 MTK update procedure

The MTK is delivered to the UE as in 6.3.2.3.1 but the MIKEY ACK is not used.

The BM-SC shall compress the NAF ID before placing it into the IDi field.

NOTE: The exact compression mechanism of NAF ID is specified in stage 3.

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

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

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 NAF 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.

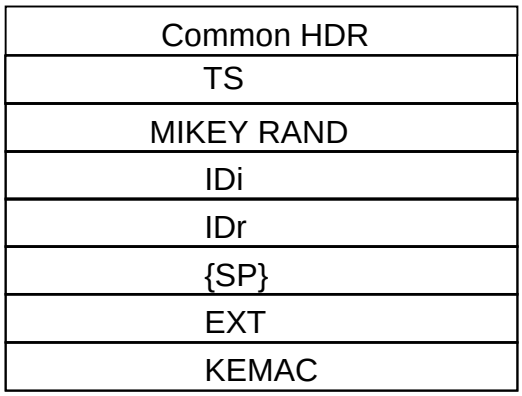

Figure 6.5: The logical structure of the MIKEY message used to deliver MSK. For use of brackets, cf. section 1.3 of RFC 3830 [9] (MIKEY)

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

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of RFC 3830 [9]).

1. ~~1.~~ The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MTSK delivery, the MSK ID is extracted from the Extension Payload.

2. The compressed NAF ID is extracted from IDi field and decompressed to NAF ID.

3~~2~~. The Timestamp Payload is checked, and the message is discarded if the counter is larger or equal to the current MIKEY replay counter associated with the given MSK (the counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than´´ should be in the sense of RFC 1982 [10].

4~~3~~. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message shall be discarded.

5~~4~~. The MTK message and NAF_ID ~~is~~ are transported to MGV-F for further processing, cf 6.5.3.

6~~5~~. The MGV-F replies success (i.e. sending the MTK) or failure.

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

6.5.4 MTK validation and derivation

When the MGV-F receives the MIKEY message and NAF ID, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, 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 number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is 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. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC as defined in RFC 3830 [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. If the MAC verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the MAC verification is successful, then the MGV-F shall update SEQs with SEQp value and start the generation of MTK. The MGV-F provides the MTK to the ME.

The MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

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).

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

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 ME also includes in this request NAF_Id 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 ~~Network~~ NAF ID, Key Group ID, MSK ID, MSK and MSK Validity Time (in the form of MTK ID interval).

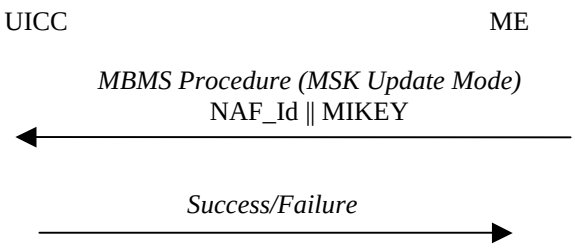

Figure D.1: MSK Update Procedure

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

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, ~~Network~~ NAF ID, Key Group ID, MSK ID, MTK ID = SEQp, MSK_C[MTK] and MAC). After performing some validity checks and decompressing the NAF_ID, the ME sends the whole message and NAF ID 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.

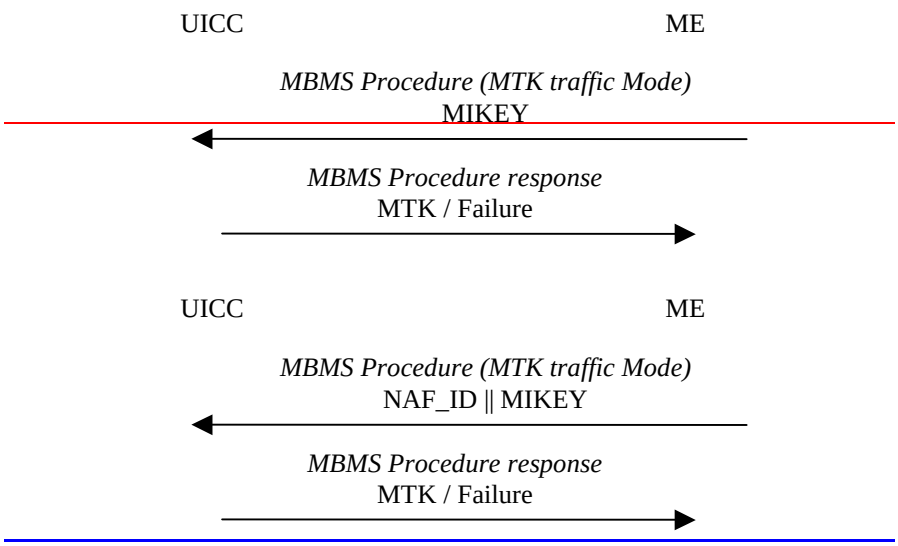

Figure D.3: MTK Generation and Validation