3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010084**

13 September, 2001

Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#19 **S3-010390**

3 - 6 July, 2001, Newbury, UK (Rev. of S3-010327)

Agenda Item: 7.1
Source: Ericsson / Siemens Atea
Title: Overview on MAP Security procedures
Document for: Discussion and decision

1. Scope and objectives

The main objective of this document is to define the mechanisms and flows for the protection of MAP signaling within 3GPP Rel4.

Some open issues for discussion during S3#19 are also brought up.

2. Introduction

According to latest agreements in S3, the support of automatic key exchange will not be provided as part of the security architecture defined for protection of MAP messages during Rel4 (key negotiation and distribution shall be performed by other means).

This document proposes the process on how MAP-NEs shall trigger the MAPsec functionality in an step-by-step approach that hopefully serves as an overview of the MAPsec feature that could be included in MAPsec specification TS 33.200.

For the sake of comprehension and readability, it might be useful to set clear some definitions used in this contribution:

- **MAPsec message**:
  A MAP message that has been protected using the security mechanisms defined in TS 33.200 (confidentiality, integrity and anti-reply protection).
  Talking in stage 3 jargon, it will be a MAP message sent within a MAP dialogue identified by an application context ‘secureTransportHandling’; synonymous for MAPsec message with PM0, PM1 or PM2
- **Unprotected MAP message**:
  A MAP message that does not implement any of the security mechanisms defined in TS 33.200 (confidentiality, integrity and anti-reply protection) which basically means a MAP message without Security Header.
  Talking in stage 3 jargon, it will be a MAP message sent within a MAP dialogue identified by an application context (TS 29.002) different from ‘secureTransportHandling’.

3. MAP Security Overview

3.1. General Overview

Imagine a network scenario with two MAP-NEs at different PLMNs (NEa and NEb) willing to communicate using MAPsec. Figure 1 presents the proposed procedure.

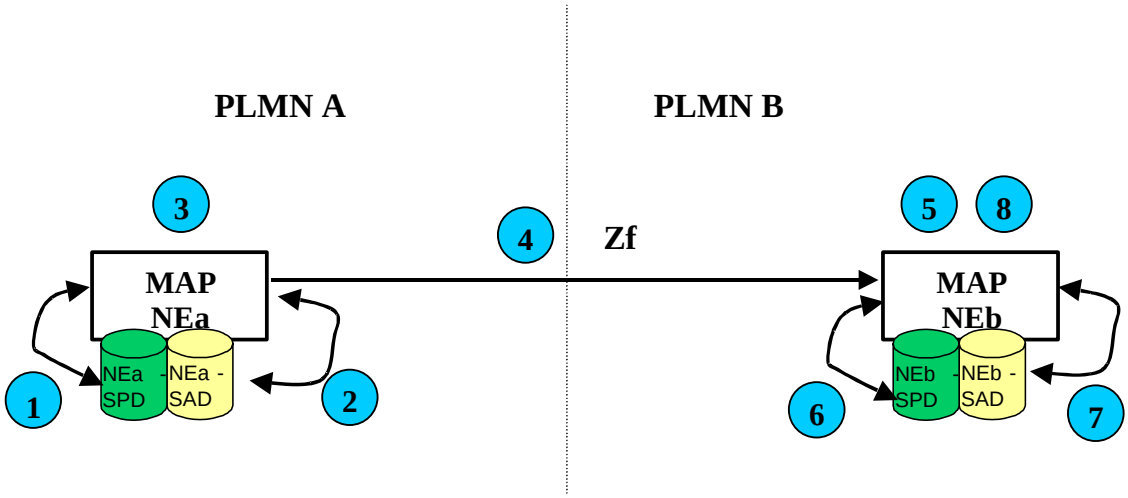

Figure 1. MAPsec Message Flow

According to Figure 1, when MAP-NEa (NEa) from PLMN A wishes to communicate with a MAP-NEb (NEb) of PLMN B using MAP protocol, the process is the following:

As the Sending Entity, NEa performs the following actions during the outbound processing of every MAP message:

1. NEa checks its Security Policy DataBase (SPD) to check if MAP security mechanisms shall be applied towards PLMN B:
   a) If the SPD does not mandate the use of MAPsec towards PLMN B, then normal MAP communication procedures will be used and the process continues in Step 4.b.
   b) If the SPD mandates the use of MAPsec towards PLMN B, then the process continues at step 2.
   c) If no valid entry in the SPD is found for PLMN B, then the communication is aborted and an error is returned to higher protocol layers.
2. NEa checks its Security Association Database (SAD) for a valid Security Association (SA) to be used towards PLMN B.
   a) In case protection of MAP messages towards PLMN B is not possible (e.g. no SA available, invalid SA…), then the communication is aborted and an error is returned to higher protocol layers.
   b) If a valid SA exists BUT the MAP dialogue being handled does not require protection (Protection Mode 0 applies to all the components of the

dialogue), then the original MAP message in cleartext can be sent in step 4.b.

c) If a valid SA exists and the MAP dialogue being handled requires protection, then the process continues at step 3.

In the case where more than one valid SA is available at the SAD, NEa shall choose the one expiring the sooner.

3. NEa constructs MAPsec message using the parameters (keys, algorithms and protection profiles) found in the SA towards PLMN B

4. NEa generates either:

a) MAPsec traffic towards NEb.

b) An unprotected MAP message in the event that the SPD towards NEb or protection profiles for that specific MAP dialogue so allows it (1.a. or 2.b.).

As the Receiving Entity, NEb performs the following actions during the inbound processing of every MAP message received:

5. If an unprotected MAP message is received, the process continues with Step 6.

Otherwise, NEb decomposes the received MAPsec message and retrieves basic information to apply security measures ('SPI', 'sending PLMN-ID', 'TVP', 'IV' and 'Original Component Identifier').

Freshness of the protected message shall be also checked at this time. If the Time Variant Parameter (TVP) received in the protected message is out of the acceptable window then the message shall be discarded.

6. NEb then checks its SPD:

a) If an unprotected MAP message was received and the SPD does not mandate the use of protected MAP messages, then the unprotected MAP message received is simply processed.

Note: Here we have the problem discussed at S3#18. If an unprotected message is received, NEb can not properly address the SPD (policy check during 6.a. and 6.b.) and the SAD (profile check during 7.a. and 7.b.) since SendingPLMNId and SPI are missing!

It shall be explicitly noted that it is out of the scope of this contribution to propose a solution to this problem. This shall be done in separate contributions being therefore the flows proposed in this contribution affected by the solution adopted afterwards.

b) If an unprotected MAP message was received BUT the SPD mandates the use of MAPsec messages, then the process continues in step 7.

Note: SA needs to be checked in case Protection Profile might allow that this specific message is unprotected.

c) If a MAPsec message was received, BUT the SPD indicates that MAPsec is NOT to be used, then the message is discarded and an error is reported to higher protocol layers.

If the MAP dialogue is still open and it is waiting for an answer, NEb also reports this error condition back to NEa.

d) If a MAPsec message was received and the SPD indicates that MAPsec is required, then the process continues at step 7.

e) If no valid entry in the SPD is found for PLMN A, then the message is discarded and an error is reported to higher protocol layers.

   If the MAP dialogue is still open and it is waiting for an answer, NEb also reports this error condition back to NEa.

7. NEb checks its SAD:

   a) If an unprotected MAP message was received, SPD mandated protection BUT SA indicates that the MAP dialogue being handled does not require protection (Protection Mode 0 applies to all the components of the dialogue), then the unprotected MAP message received is simply processed.

   b) If an unprotected MAP message was received, SPD mandated protection and SA indicates that the MAP dialogue being handled requires protection, then NEb checks whether “Fallback to Unprotected Mode” is allowed:

      - If NOT allowed, then the message is discarded and the corresponding error is reported to higher protocol layers.

        If the MAP dialogue is still open and it is waiting for an answer, NEb also reports this error condition back to NEa.

      - If allowed, then the unprotected MAP message received is simply processed.

   c) If a MAPsec message was received, SPD mandated protection and the received SPI points to a valid SA, then the process continues at step 8.

   d) If the received SPI does not point to a valid SA, the message is discarded and an error is reported to higher protocol layers.

      If the MAP dialogue is still open and it is waiting for an answer, NEb also reports this error condition back to NEa.

8. Integrity and encryption mechanisms are applied on the message as per the information in the SA (Keys, algorithms, protection profiles).

   a) If the result after applying such procedures is NOT successful then the message is discarded and an error is reported to higher protocol layers.

      If the MAP dialogue is still open and it is waiting for an answer, NEb also reports this error condition back to NEa.

   b) If the result after applying such procedures is successful, then NEb has the cleartext message NEa originally wanted to send NEb. After this, the MAP communications found inside the MAPsec headers are processed normally.

In the event the received message at NEb requires an answer to NEa (Return Result/Error), NEb will perform the process in steps 1 to 4 acting as the Sender and NEa will perform the process in steps 5 to 8 acting as the Receiver.

3.2. Fallback to Unprotected Mode

In early stages of deployment of MAPsec, it might be the case that not every NE within a PLMN implements MAPsec at the same point of time. Fallback to Unprotected Mode is allowed in these scenarios.

How Fallback to Unprotected Mode is achieved when a MAPsec enabled NE receives an unprotected message from a non-MAPsec enabled NE has been already specified above (Step 7.b.).

In the event a MAPsec enabled NE initiates a secured MAP communication towards a non-MAPsec enabled NE, the MAPsec enabled NE will receive an error indication of such circumstance (i.e. “OperationNotSupported”). When this occurs, the MAPsec enabled NE shall check whether “Fallback to Unprotected Mode” is allowed:

- If NOT allowed, then the communication is aborted.
- If allowed, then the MAPsec enabled NE could send an unprotected MAP message instead.

4. Issues for Discussion

In this section, some issues for discussion raised while the preparation of this contribution are brought to the attention of the rest of S3.

4.1 Handling of Error Conditions

It has been proposed in this contribution that NEb reports error conditions back to NEa. The error conditions are reported when:

- Valid entry in SPD not available.
- Valid entry in SAD not available.
- Protection applied not adequate.

Although from a security point of view it might not be recommendable to send this kind of indications, it is the understanding of the authors of this contribution that it would help to identify pure operational errors (mismatch in SPD and SAD at peer NEs) especially during Rel4 where SPDs and SADs will have to be managed by manual procedures.

Moreover, in some cases the notification of error conditions will be required by the MAP protocol itself in order to close the MAP dialogue.

Another issue that can be raised under this point is whether such error conditions are already considered in N4 specification and how problematic it would be for them to consider them otherwise.

4.2 Fallback to Unprotected Mode

It is the understanding of the authors of this contributions that Fallback to Unprotected Mode shall be only allowed in deployments scenarios when some of the NEs in the peer PLMN might not implement MAPsec.

This implies that NEa shall NOT perform checking of Fallback to Unprotected Mode Indicator when any other error condition apart from “MAPsec not supported” (“OperationNotSupported”) is reported.

4.3 Checking SPD for Unprotected Messages

This contribution proposes how unprotected messages shall be dealt with when received by NEb. However and as already discussed at S3#18, from a practical point of view we face the problem that it will not be possible for NEb to properly address the SPD and SAD since unprotected MAP messages do not contain a Security Header which transports the SendingPLMN-Id and SPI.

Possible solutions to this problem shall be discussed at S3#19. The agreed solution might influence the flows proposed in this contribution on the basis of the current understanding of the TS 33.200.

5. Conclusion

S3 members are kindly asked to consider the proposed flows for MAPsec messages proposed in this contribution in order to hopefully agree on them and incorporate such information into TS 33.200.

Hopefully this proposal also serves as a framework to discuss the Open issues raised in this contribution. As a result of these discussions, the flows presented here might be affected in order to accommodate the agreed solution.

Finally, N4 shall be informed of agreements and open issues after the discussion of this contribution looking for alignment between Stage 2 TS 33.200 and Stage 3 TS 29.002.