Technical Specification Group Services and System Aspects
Meeting #14, Kyoto, Japan, 17-20 December 2001

***TSGS#14(01)0619***

**Source:** **SA WG3**

**Title:** **1 CR to 33.200: Removing the Sending PLMN-Id from Security Header (Rel-4)**

**Document for:** **Approval**

**Agenda Item:** **7.3.3**

| Spec | CR | Rev | Phase | Cat | Subject | Version-Current | Version-New | Doc-2nd-Level |
|---|---|---|---|---|---|---|---|---|
| 33.200 | 017 | | Rel-4 | F | Removing the Sending PLMN-Id from Security Header | 4.1.0 | 4.2.0 | S3-010658 |

**3GPP TSG SA WG3 Security — S3#20** **S3-010658**

**27 - 30 November, 2001**

**Sophia Antipolis, France**

*CR-Form-v4*

# CHANGE REQUEST

⌘ **33.200** **CR** **017** ⌘ ev **-** ⌘ Current version: **4.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Removing the Sending PLMN-Id from Security Header |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | SEC1-MAP |
| ***Date:*** | ⌘ | 26-11-01 |
| ***Category:*** | ⌘ | **F** |
| ***Release:*** | ⌘ | Rel-4 |

*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)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | To explicitly avoid a security weakness, take the redundancy out of the security header and specify how the 'Original Component Identifier' is used |
| ***Summary of change:*** | ⌘ | 1) The possibility of faking the 'Sending PLMN-Id' is explicitly removed<br>2) The way 'Original Component Identifier' is used in processing MAP messages is clarified<br>3) Unnecessary data is removed from the security header to reduce signalling overhead |
| ***Consequences if not approved:*** | ⌘ | A security weakness may be left in MAPsec and the inbound message processing will be left incomplete |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.5.1, Annex B |
| ***Other specs affected:*** | ⌘ | ☐ Other core specifications ⌘ TS 29.002<br>☐ Test specifications<br>☐ O&M Specifications |
| ***Other comments:*** | ⌘ | |

********** First Changed Section **********

## 5.5.1 MAPsec security header

For Protection Mode 0, t~~T~~he security header is a sequence of the following data elements:

*Security header = ~~TVP || NE-Id || Prop || Sending PLMN-Id ||~~ SPI || Original component Id*

For Protection Modes 1 and 2, the security header is a sequence of the following elements:

*Security header = SPI || Original component Id || TVP || NE-Id || Prop*

- **Security Parameters Index (SPI):**

  SPI is an arbitrary 32-bit value that is used in combination with the Destination PLMN-Id to uniquely identify a MAP-SA.

- **Original component Id:**

  Identifies the type of component (invoke, result or error) within the MAP operation that is being securely transported (Operation identified by operation code, Error defined by Error Code or User Information).

- **TVP:**

  The TVP is used for replay protection of Secured MAP operations is a 32 bit time-stamp. The receiving network entity will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived is 0.1 seconds. The size of the time-window at the receiving network entity is not standardised.

- **NE-Id:**

  6 octets used to create different IV values for different NEs within the same TVP period. It is necessary and sufficient that *NE-Id* is unique per PLMN. (This is sufficient because sending keys are unique per PLMN.) The NE-Id shall be the E.164 global title of the NE without the MCC and MNC.

- **Proprietary field (PROP):**

  4 octets used to create different IV values for different protected MAP messages within the same TVP period for one NE. The usage of the proprietary field is not standardised.

~~- **Sending PLMN-Id:**~~

~~PLMN-Id is the ID number of the sending Public Land Mobile Network (PLMN). The value for the PLMN-Id is a concatenation of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the sending network.~~

~~- **Security Parameters Index (SPI):**~~

~~SPI is an arbitrary 32-bit value that is used in combination with the sender's PLMN-Id to uniquely identify a MAP-SA.~~

~~- **Original Component identifier:**~~

~~Identifies the type of component (invoke, result or error) within the MAP operation that is being securely transported (Operation identified by operation code, Error defined by Error Code or User Information).~~

********** Second Changed Section **********

# Annex B (normative): MAPsec message flows

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

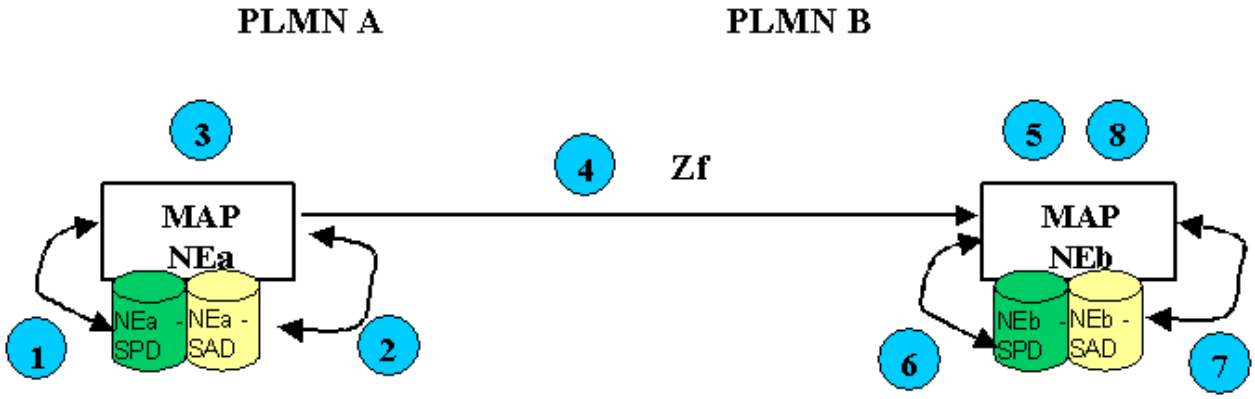


**Figure 1. MAPsec Message Flow**

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 the MAP user.

2. NEa checks its Security Association Database (SAD) for a valid Security Association (SA) to be used towards PLMN B. In the case where more than one valid SA is available at the SAD, NEa shall choose the one expiring the sooner.

   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 MAP user.

   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 either the original MAP message in cleartext is sent in step 4.b, or a MAPsec message with Protection Mode 0 is created in step 3.

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

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

4. NEa generates either:

   a) MAPsec message 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.).

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

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

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

   ~~Freshness of the protected message is 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 and an error is returned to MAP user. No error message is returned to NEa.~~

6. NEb checks the SPD:

   An unprotected MAP message is received:

   a) If an unprotected MAP message is received and fallback to unprotected mode is allowed, then the unprotected MAP message is simply processed (Process goes to END)

   b) If an unprotected MAP message is received and the 'MAPsec operation components table' of the SPD does not mandate the use of MAPsec for the included 'Original Component Identifier', then the unprotected MAP message is simply processed (Process goes to END)

   c) If an unprotected MAP message is received, the 'MAPsec operation components table' of the SPD mandates the use of MAPsec for the included 'Original Component Identifier' and fallback to unprotected mode is NOT allowed, then the message is discarded.

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

   A MAPsec message is received, NEb checks SPI in the SPD:

   d) If SPI is not in SPD or there is no valid entry for the PLMN associated with SPI in the SPD ~~is found for PLMN A~~, then the message is discarded and an error is reported to MAP user.

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

   e) If a MAPsec message is received, but the SPD indicates that MAPsec is NOT to be used, then the message is discarded and an error is reported to MAP user.

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

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

7. NEb checks its SAD to retrieve the relevant SA-information for processing of the MAPsec message:

   a) If the received SPI points to a valid SA, then NEb uses the 'Original Component Identifier' in the MAPsec header to identify the protection mode that has to be applied to the component indicated, according to the protection profile indicated in the SA. If Protection Mode 0 was applied, then the MAP message is simply processed (Process goes to END). Otherwise the process continues at step 8.

   b) If the received SPI does not point to a valid SA, the message is discarded and an error is reported to MAP user. If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

8. Freshness of the protected message is checked by ensuring the Time Variant Parameter (TVP) is in an acceptable window. Integrity and encryption mechanisms are applied ~~on~~ to the message according to the identified protection mode, by using the information in the SA (Keys, algorithms~~, protection profiles~~).

   a) If the result after applying such mechanisms is NOT successful then the message is discarded and an error is reported to MAP user. If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

   b) If the result after applying such procedures is successful, then NEb has the cleartext MAP message NEa originally wanted to send NEb. The cleartext MAP message can now be processed (Process goes to END)

END: A cleartext MAP message is available at NEb.

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.

In the event a MAPsec enabled NE initiated a secured MAP communication towards a non-MAPsec enabled NE and the MAPsec enabled NE received an error indication of such circumstance (i.e. "ApplicationContextNotSupported"). 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 shall send an unprotected MAP message instead.

The same procedures shall apply to secure MAP communications between MAP-NEs in the same PLMN.

NOTE: Because various error cases may be caused by active attacks, it is highly recommended that the cases are reported to the management system.