3GPP TSG SA WG3 Security — S3#20 **S3-010606**
27 - 30 November, 2001
Sophia Antipolis, France

CR-Form-v4

CHANGE REQUEST

⌘ **33.200 CR** ⌘ 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 ☒

Title:	⌘	Removing the Sending PLMN-Id from Security Header		
Source:	⌘	Hutchison 3G UK		
Work item code:	⌘	MAPsec	***Date:*** ⌘	22-11-01
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 and take the redundancy out of the security header
Summary of change:	⌘	Unnecessary data is removed from the security header and the possibility of faking the Sending PLMN-Id is removed
Consequences if not approved:	⌘	A security weakness may be left in MAPsec

Clauses affected:	⌘	5.5.1, Annex B		
Other specs affected:	⌘	□ Other core specifications	⌘	TS 29.002
		□ Test specifications		
		□ 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 Mode 1 or 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 (OCI):**

  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.

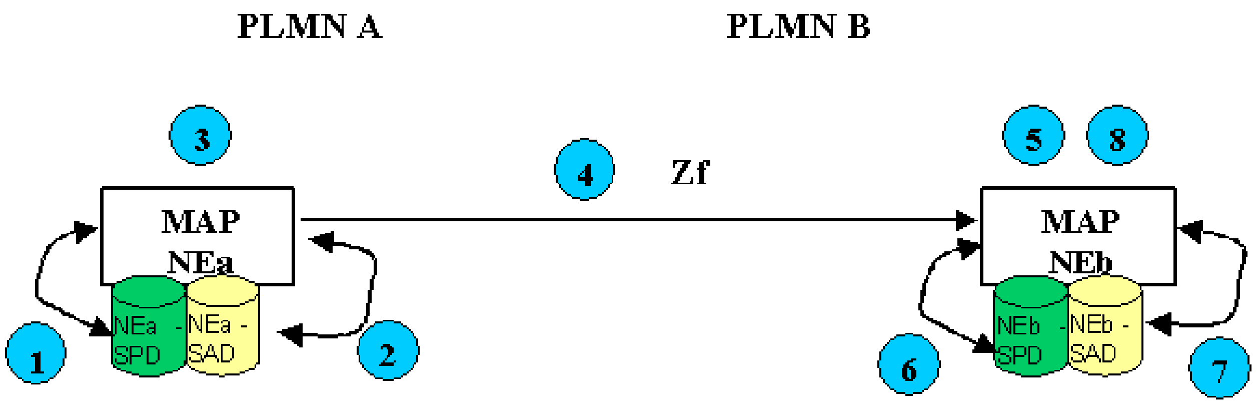

Figure 1. MAPsec Message Flow

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.

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 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. ~~Integrity and encryption mechanisms are applied on the message using the information in the SA (Keys, algorithms, protection profiles).~~NEb uses tha SA and OCI to work out the protection mode applied to the message and undoes any encryption, performs any integrity check and ensures that TVP is in an acceptable window as appropriate.

   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.

3GPP TSG SA WG3 Security — S3#20 **S3-010606_attachment**

27 - 30 November, 2001

Sophia Antipolis, France

3GPP TSG CN WG4 Meeting #11 ***N4-011374***

Cancun, Mexico, 26th - 30th November 2001

CR-Form-v5

CHANGE REQUEST

⌘ **29.002 CR** ⌘ **rev** **-** ⌘ Current version: **4.5.0** ⌘

*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: ⌘	Aligning the security header elements with TS33.200			
Source: ⌘	Hutchison 3G UK			
Work item code: ⌘	TEI-4		***Date:*** ⌘	21-11-2001
Category: ⌘	**F**		***Release:*** ⌘	REL-4
	Use <u>one</u> 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 <u>one</u> 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 align 29.002 with TS 33.200. Changes in SA3 have been made to remove redundancy in the security header.
Summary of change: ⌘	Security header elements are modified to remove two existing elements (Initialisation Vector and Sending PLMN Identity) and add three optional elements (TVP, NE-Id, Prop). These new elements contain similar information to the Initialisation Vector.
Consequences if not approved: ⌘	Specifications are not aligned and interoperability may be affected.

Clauses affected: ⌘	7.6.12.1		
Other specs affected: ⌘	□ Other core specifications	⌘	TS33.200
	□ Test specifications		
	□ O&M Specifications		
Other comments: ⌘			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

7.6.12 Secure Transport Parameters

7.6.12.1 Security Header

This parameter carries the security header information, which is required by a receiving entity in order to extract the protected information from a securely transported MAP message. The components of the security header are shown in table 7.6.12/1.

See 3GPP TS 33.200 for the use of these parameters.

Table 7.6.12/1: Components of the Security Header

Component name	Presence requirement	Description
~~Initialisation vector~~	~~M~~	~~An initialisation vector for the message protection function. The TVP part of the IV is mandatory. The other parts shall be present if required for the current Protection Mode.~~
~~Sending PLMN identity~~	~~M~~	~~The Mobile Country Code and the Mobile Network Code of the PLMN which sent the secure MAP message.~~
Security Parameters Index	M	Identifies the Security Association for the component.
Original component identifier	M	Identifies the type of component to be securely transported – one of: - Operation, identified by the operation code; - Error, defined by the error code; - User information.
TVP	O	A parameter based on time that is used to ensure the current message is fresh. This is only present if required for the current Protection Mode.
NE-Id	O	The identity of the Network Element sending the message. This is only present if required for the current Protection Mode.
Prop	O	Bytes used to ensure the IV is unique for a given TVP and NE-Id. This is only present if required for the current Protection Mode.