3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010114**

13 September, 2001, Sophia Antipolis, France

CR-Form-v4

CHANGE REQUEST

⌘	**33.200**	**CR**	**XXX**	⌘	ev	**-**	⌘	Current version:	**4.0.0**	⌘

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

Proposed change affects: ⌘ (U)SIM □ ME/UE □ Radio Access Network □ Core Network ☒

Title:	⌘	Moving Sending PLMN-Id to the SA from the security header		
Source:	⌘	Hutchison 3G UK		
Work item code:	⌘	MAPsec	***Date:*** ⌘	29-06-2001
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 remove a security weakness and take the rundancy out of the security header
Summary of change:	⌘	Sending PLMN-Id is added an SA and unnecessary elements of the security header are removed
Consequences if not approved:	⌘	A security hole will be left in MAPsec

Clauses affected:	⌘	5.4, 5.5.1		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘			

5.4 MAPsec security association attribute definition

The MAPsec security association is a sequence of the following data elements:

MAPsec security association = Sending PLMN-ID || MEA || MEK || MIA || MIK || PPI || Fallback || SA lifetime

- 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.

- MAP Encryption Algorithm identifier (MEA):

Identifies the encryption algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. Mapping of algorithm identifiers is defined in clause 5.6.

- MAP Encryption Key (MEK):

Contains the encryption key. Length is defined according to the algorithm identifier.

- MAP Integrity Algorithm identifier (MIA):

Identifies the integrity algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. Mapping of algorithm identifiers is defined in section 5.6.

- MAP Integrity Key (MIK):

Contains the integrity key. Length is defined according to the algorithm identifier.

- Protection Profile Identifier (PPI):

Identifies the protection profile. Length is 16 bits. Mapping of profile identifiers is defined in section 6.

- Fallback to Unprotected Mode Indicator (FALLBACK):

In the case that protection is available, this parameter indicates whether fallback to unprotected mode is allowed. This is a one bit indicator where the value one indicates that fall back to unprotected mode is permitted and value zero indicates that fallback to unprotected mode is not permitted.

Editor’s note: The fallback indicator may be moved to the SPD.

- SA Lifetime:

Defines the actual expiry time of the SA. The expiry of the lifetime shall be given in UTC time.

Editor’s Note: The exact format and length to be defined.

If the SA is to indicate that MAPsec is not to be applied then all the algorithm attributes shall contain a NULL value.

5.5 MAPsec structure of protected messages

MAPsec provides for three different protection modes and these are defined as follows:

Protection Mode 0:	No Protection
Protection Mode 1:	Integrity, Authenticity
Protection Mode 2:	Confidentiality, Integrity, and Authenticity

MAP operations protected by means of MAPsec consist of a Security Header and the Protected Payload. Secured MAP messages have the following structure:

Security Header	Protected Payload

In all three protection modes, the security header is transmitted in cleartext.

In protection mode 2 providing confidentiality, the protected payload is essentially the encrypted payload of the original MAP message. For integrity and authenticity in protection modes 1 and 2, the message authentication code is calculated on the security header and the payload of the original MAP message in cleartext and it is included in the protected payload. In protection mode 0 no protection is offered, therefore the protected payload is identical to the payload of the original MAP message.

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 1 or 2, the security header is a sequence of the following data 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 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).

- **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).~~