3GPP TSG SA WG3 Security — S3#20 **S3-010498**

16 - 19 October, 2001

Sydney, Australia

Source: **Hutchison 3G UK**

Title: **Some potential changes for MAPsec**

Document for: **Discussion/Decision**

Agenda Item: **7.1 MAP security**

This contribution contains several suggestions for changes to TS 33.200. It is requested that SA3 make a decision on each of the possible changes, in order that the relevant CRs can be prepared.

Checking the Sending PLMN-Id from the security header

In the current message flow, the receiving entity never checks the sending PLMN-Id given in the security header against anything and hence assumes it is correct. This causes a security weakness in that the sender of a message can put any valid sending PLMN-Id (i.e. one the receiver will recognise) in the security header. This has the affect of fooling MAP layer into believing the message has actually come from a different PLMN that it actually has and will cause the receiving entity to respond with an SA that is towards a different PLMN.

This weakness is easy to avoid. It can be done by checking the combination of SPI and sending PLMN-Id given in the security header against the combination held in either the SPD or SAD. The most natural place for this to happen is in the SPD. If it happens in the SAD, sending PLMN-Id needs to be added to each SA (a good idea anyway in my opinion).

This would require a change to the message flow along the lines of the following

A MAPsec message is received, NEb checks SPI and sending PLMN-Id in SPD:

d) If no valid entry in the SPD is found for PLMN A or the given SPI is not an SA 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) ……

In fact the sending PLMN-Id in the security header adds no value, as it needs to be checked. It is also uniquely identified by the combination of destination PLMN-Id and SPI (recall this uniquely identifies an SA). Removing the sending PLMN-Id from the security header would require a change to the message flows along the lines of the following:

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) ….

Removing the sending PLMN-Id form the security header will save redundancy from every message sent using MAPsec. This will also require a change in TS 29.002, which requires a change to align with TS 33.200 anyway (see below).

This contribution proposes removing the Sending PLMN-Id from the security header, as it is purely redundant information. It also proposes altering the message flow to plug a security weakness.

Protection Mode 0 Security Headers

TVP, NE-Id and Prop are not used to process a MAP message transmitted with Protection Mode 0. These means there are 14 unused bytes transmitted.

Therefore it is proposed to remove TVP, NE-Id and Prop from the security header of Protection Mode 0 messages.

SA Identifiers

As an SA is uniquely identified by a destination PLMN-Id and an SPI (TS 33.200 v4.1.0, page 9), it seems sensible that the destination PLMN-Id and the SPI should be included in the SA.

This contribution proposes adding destination PLMN-Id and SPI to the SA. It also proposes that sending PLMN-Id is included in the SA for completeness.

Alignment of TS 29.002 and TS 33.200

Pages 87/88 of v4.5.0 of TS 29.002 contains the following

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.

Page 9 of v4.1.0 contains the following:

5.5.1 MAPsec security header

The security header is a sequence of the following data elements:

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

These are clearly out of alignment as TS 29.002 thinks Prop and NE-Id are optional, whereas TS 33.3200 thinks they are mandatory. This contribution proposes creating a CR to re-align TS 29.002 with TS 33.200 taking into account any changes suggested by this document that are agreed.

Preparation of resulting CRs

Hutchison will undertake to prepare the relevant CRs for SA3 and CN4 resulting from this contribution.