3GPP TSG SA WG3 Security — S3#20 **S3-010528**

16-19 October, 2001 **(revised S3-010426)**

Sydney, Australia

Source: **Huawei Technologies CO., LTD/CWTS**

Title: Proposed Updates to Structures of SADB and SPD on MAPSec

Document for: Discussion / Decision

Agenda Item:

1. Abstract

This contribution proposes that PPI should be moved from SADB to SPD and SPI should be a mandated parameter in SADB.

2. Analysis

2.1 Architectures of SA, SP and MAPSec header

Recently, S3-010352 from Alcatel proposes that:

(1) A MAPSec SPD entry must contain three parameters, which are **Target PLMN_id**, **Fallback** and **a SA pointer** to the MAP SA entries in the SADB.

(2) A MAPSec SADB entry must contain six parameters, which are **MEA**, **MEK**, **MIA**, **MIK**, **PPI** and **SA lifetime**.

Notes: this proposal had been approved in SA3#19 meeting.

In TS 33200 V400, the security header is a sequence of the following data elements:

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

2.2 Moving PPI from SADB to SPD

S3-010390 from Ericsson / Siemens provides a simple overview about MAP security. The basic mechanism is as the following figure 1.

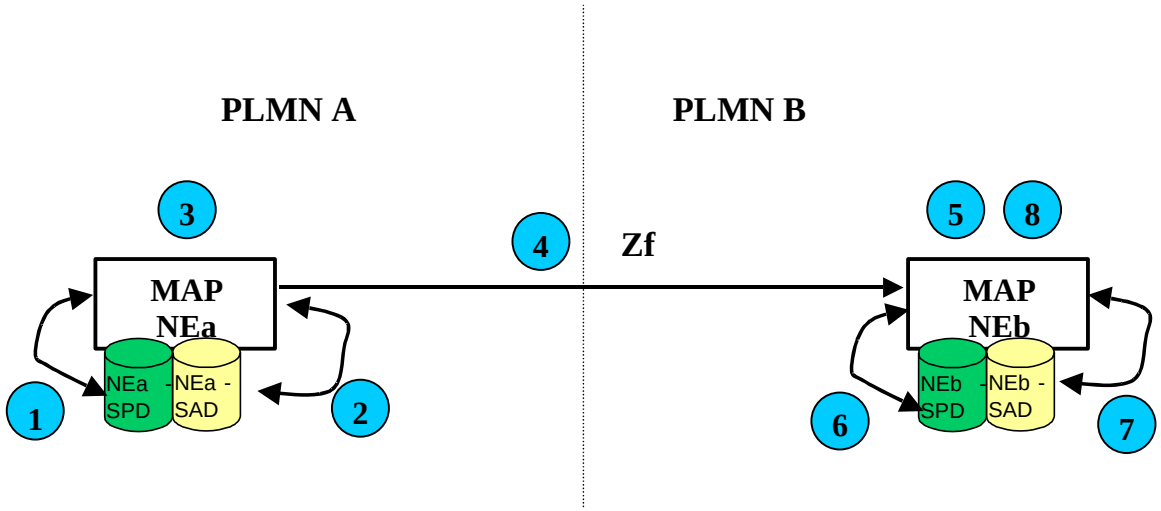

Figure 1. MAPSec Message Flow (From S3-010390)

But there are two problems in S3-010390:

(1) **In Step 1**: Which parameter in SPD is used by NEa to determine whether the MAPSec protection shall be applied on a MAP message towards PLMN B?

(2) **in Step 6**: Which parameter in SPD is used by NEb to determine whether a received MAP or MAPSec message abide by the security policy rule between PLMN A and B?

It is well known that only PPI (Protection Profile Index) is used for indicating the protection fashion for the MAP messages. PPI is used to indicate the protection granularity of MAP, which is based on operational component level. But unfortunately, all three parameters (**Target PLMN_id**, **Fallback** and **a SA pointer**) contained in MAPSec SPD entry cannot directly indicate what is the protection policy (Protection Profile) of a sending / received MAP message. It is only PPI in SADB that can do it.

Consequently, the searching PPI procedure for NE is as the following:

(1) In step1: The NEa must search for a security policy entry in SPD by used of **Target PLMN_id**, and then search for the corresponding SA from SADB according to **a SA pointer** in SPD and take the PPI parameter from SA.

(2) In step6: If a MAPSec message is received, NEb may find the PPI parameter from SADB by used of SPI in MAP security header. If a MAP message is received, NEb needs to do the same procedure as in step 1.

We suggest that PPI should be moved from SADB to SPD (i.e., PPI is a mandated parameter in SPD instead of SADB), which will introduce the following benefits:

(1) *More simple and faster for the searching PPI procedure in step 1 and 6*.

It is unnecessary for NE to search for the PPI parameter in SADB by used of a SA pointer in SPD.

(2) *Reducing the space size of SADB*.

PPI is a parameter used for security policy. It should not be a parameter of SADB.

So it is suggested that PPI should be moved from SADB to SPD.

2.3 Adding SPI to SADB

Security Parameter Index (SPI) is an index, which is used to help NE to indicate a unique SA for an incoming MAPSec message. So SADB must contain SPI parameter.

3. Conclusions

This paper suggests that PPI should be moved from SADB to SPD and SPI should be a mandated parameter in SADB.

3GPP TSG SA WG3 Security — S3#20 **S3-010528_attachment**

16-19 October, 2001

Sydney, Australia

CR-Form-v3

CHANGE REQUEST

⌘ **33.200** **CR** **CR-Num** ⌘ rev **-** ⌘ 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:	⌘	Proposed Updates to Structures of SADB and SPD on MAPSec
Source:	⌘	Huawei Technoligies CO. LTD / CWTS
Work item code:	⌘	Security ***Date:*** ⌘ 24/07/2001
Category:	⌘	**F** ***Release:*** ⌘ R4

Use one of the following categories:
- ***F*** *(essential 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:	⌘	The reason for moving PPI from SADB to SPD: (1) It is more simple and faster searching for PPI from SPD than from SADB. It is unnecessary for MAP-NEs (a sender or a receiver) to search for PPI parameter in SADB by use of a SA pointer in SPD. (2) The structure of SPD and SADB seems more reasonable. The SADB is variable when some SAs expire, and the SPD is relatively invariable after the security policies being decided or MAP-NEs being initialized. It is well known that PPI is a relative invariable parameter when MAP-NEs is initialised.
Summary of change:	⌘	Move PPI from SADB to SPD
Consequences if not approved:	⌘	It is more complexity to implement and the structure of SADB and SPD seems unreasonable.

Clauses affected:	⌘	5.3 Policy requirements for the MAPsec SPD 5.4 MAPsec security association attribute definition
Other specs	⌘	☐ Other core specifications ⌘

Affected:	☐ 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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 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.

5.3 Policy requirements for the MAPsec SPD

The security policies for MAPsec key management are specified in the NE's SPD. SPD entries define which MAP SAs (if any) to use to protect MAP signalling based on the PLMN of the peer NE. There can be no local security policy definitions for individual NEs. Instead, SPD entries of different NE within the same PLMN shall be identical.

In order to enable the NE to determine which MAP SAs to use, an SPD entry must contain the following information:

- The PLMN identifier of the peer PLMN with which this policy applies. This identifier is used to select the correct policy and hence determine which MAP SA must be used when protecting MAP signalling with a peer NE.

- The fallback to unprotected mode indicator. In the case that protection is available and hence at least some MAP operations are protected under protection mode 1 or 2 with this peer PLMN, this parameter indicates whether fallback to unprotected mode is allowed.

- A pointer to the MAP SA entries, in the SAD, defined for this policy entry. There may be more than one existing MAPsec SA at a given moment due to renewal of MAPsec SAs (e.g. a new SA has been defined prior to the expiry of the old one in order to avoid disrupting the traffic when the old one expires). Nevertheless, only one MAPsec SA is to be used at a given moment. This should be the one that expires the sooner.

- Protection Profile Indicator (PPI) indicates how MAP operations over Zf-interface shall be protected, i.e., whether a MAP operation needs protection and the corresponding protection mode to be used. The length of PPI is 16 bits. Mapping of profile identifiers is defined in section 6.

The NE shall conceptually maintain two SPDs : one for incoming MAP traffic and one for outgoing MAP traffic.

5.4 MAPsec security association attribute definition

The MAPsec security association must contain the following data elements:

- **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.~~

- **SA Lifetime:**

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

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