3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010081**

13 September, 2001, Sophia Antipolis, France

3GPP TSG-SA3 Meeting #19 ***S3-010352***
London, UK, July 3-6 2001

CR-Form-v4

CHANGE REQUEST

⌘	**33.200**	**CR**	**005**	⌘	ev	**-**	⌘ Current version:	**1.0.1** ⌘

*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:	⌘	Clarifications in SPD and SAD contents		
Source:	⌘	Alcatel		
Work item code:	⌘	SEC1-MAPAL	***Date:*** ⌘	June 20, 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:	⌘	Uncomplete specification as editor's note requests for contributions on these topics related to SPD and SAD contents.
Summary of change:	⌘	Put fallback indicator in the policy database and detail contents of SPD
Consequences if not approved:	⌘	Specification remains uncomplete.

Clauses affected:	⌘	5.3, 5.4, new informative annex B.		
Other specs affected:	⌘	□	Other core specifications	⌘
		□	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.

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.

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

~~Editor's note: Some issues need to be investigated: Include and clarify fallback indicator; Policy for SA renewal, the need for START time, mechanism to distinguish inbound/outbound SPDs ? Implications of Protection Mode 0 differing between operators for the same type of operation (Danger of active attacker changing the source PLMN ID).~~

5.4 MAPsec security association attribute definition

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

~~*MAPsec security association = MEA || MEK || MIA || MIK || PPI || Fallback || SA lifetime*~~

- **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.

Annex A (informative): Guidelines for manual key management

A.1 Inter-domain Security Association and Key Management Procedures

Manual Inter-domain Security Association and Key Management procedures is subject to roaming agreements.

Some important parts of an inter-domain Security Association and Key Management agreement is:

- to define~~d~~ how to carry out the initial exchange of MAPsec SAs
- to define~~d~~ how to renew the MAPsec SAs.
- to define how to withdraw MAPsec SAs (including requirements on how fast to execute the withdrawal)
- to decide if fallback to unprotected mode is to be allowed
- to decide on key lengths, algorithms, protection profiles, and SA lifetime etc (MAPsec SAs are expected to be fairly long lived)

When renewing a MAPsec SA used for incoming MAP traffic, the "old" SA should be kept in the NEs until its expiry time is reached, unless the SA renewal was due to compromise of the keys of the "old" SA in which case the "old" compromised SA should immediately be removed from the SAD and no longer pointed to from the SPD in the NEs.

When renewing a MAPsec SA used for outgoing MAP traffic, the "old" SA should continue to be used by the NEs until its expiry time is reached, unless the SA renewal was due to compromise of the keys of the "old" SA in which case the "old" compromised SA should immediately be removed from the SAD and no longer pointed to from the SPD in the NEs. Note that one way to force the NEs to use a newly defined MAPsec SA is to distribute to NEs a new version of the SAD and SPD in which the old SA no longer exists but only the new SA.

To ease SA renewal, both PLMNs may decide to set up several MAPsec SAs in advance so that NEs can automatically switch from one SA to another SA when the former expires. In such a situation, the MAPsec SAs would have different expiry times. Because expiry time is expressed in absolute time, the MAPsec SA with the sooner expiry time should be considered as the first one to be used.

If an inbound MAPsec SA making use of Protection Mode 1 or 2 for certain types of operations is defined with a peer PLMN, then there should be no other inbound MAPsec SA defined with another PLMN that makes use of Protection Mode 0 for the same types of operations.

A.2 Local Security Association Distribution

Manual Local Security Association Distribution is executed entirely within one PLMN and is consequently at the discretion of the administrative authority.

The requirement on the manual distribution procedures can be summarized as follows:

- Fallback to unprotected mode. MAPsec may be **required** or it may be **optional** towards other MAP-NEs. Procedures to set this information in the MAP-NEs on a per PLMN destination basis must be provided. This information should available to the MAP-NE before any communication towards other MAP-NEs is to take place. ~~MAP-NEs capable of executing MAPsec should define a default value for the MAPsec **fallback to unprotected mode** indicator.~~
- Procedures for transporting the relevant MAPsec SA to the MAP-NEs must be defined. In order to ensure that the MAPsec SA are present when needed, all valid MAPsec SA should be distributed to all MAP-NEs as soon as they are available.
- Procedures for revocation of MAPsec SAs must be defined