3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010095**

13 September, 2001, Sophia Antipolis, France

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** ⌘ 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 **X**

Title:	⌘	Content and identifiers of a MAPSec SA
Source:	⌘	Ericsson
Work item code:	⌘	MAPsec
Date:	⌘	13-09-2001
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:	⌘	In line with other CRs presented to this meeting, this CR proposes that Fallback to unprotected mode indicator is moved from MAPSec SA to form part of the SPD instead. What is new in this CR is that definition of Fallback indicator is removed from the description of a MAPSec SA, thing that was not done in the other CRs. Additionally, it was not stated in the specification what the identifiers of a MAPSec SA were.
Summary of change:	⌘	Fallback to unprotected mode indicator is removed from content of a MAPSec SA. It is stated that PLMN-id and SPI are the identifiers of a MAPSec SA.
Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	5.3, 5.4
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications
	⌘	
Other comments:	⌘	

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.

Fallback to unprotected mode.

- Procedures to set the "fallback to unprotected mode" (enabled/disabled) in the MAP-NEs must be provided. For the receiving direction, it is sufficient to have a single parameter indicating whether fallback for incoming messages is allowed or not. For the sending direction, the information should indicate for each destination PLMN whether fallback for outgoing messages is allowed or not. This state shall be available to the MAP-NE before any communication towards other MAP-NEs can take place.
- The use of the fallback indicators is specified in Annex B.
- The security measures specified in this TS are only fully useful for a particular PLMN if it disallows fallback to unprotected mode for MAP received from any other PLMN after a certain cut-off date.

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 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.

A MAPsec SA is identified by a PLMN-Id and a Security Parameters Index, SPI:

- PLMN-Id determines the peer PLMN the MAPsec SA shall be used with.

- SPI makes possible to distinguish different kind of MAPSec SAs e.g. for inbound and outbound traffic, future SAs to be put in practice once the current one has expired, etc.

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