3GPP TSG SA WG3 Security — S3#20 **S3-010542**

16 - 19 October, 2001

Sydney, Australia

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **015** ⌘ ev **-** ⌘ Current version: **4.1.0** ⌘

*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:	⌘	Policy configuration clarification
Source:	⌘	SA WG3
Work item code:	⌘	MAPsec
Date:	⌘	09 Oct 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:	⌘	A good security practise requires the explicit inclusion of all communication partners (PLMN's) in the policy database. Within Annex B (Flows) it was already described that, when a MAPsec message is received and no valid entry in the SPD is found for PLMN A, then the message is discarded and an error is reported to MAP user.
Summary of change:	⌘	Explicit configuration requirement for the SPD is included in relevant clause 5.3.
Consequences if not approved:	⌘	Network operators not aware of this may experience MAPsec network introduction problems.

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

5.3 Policy requirements for the MAPsec Security Policy Database (SPD)

The security policies for MAPsec key management are specified in the NE's SPD. SPD entries define which MAP operation components are protected and 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:

- The "fallback to unprotected mode" (enabled/disabled) shall be available to the MAP-NE before any communication towards other MAP-NEs can take place. 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;

- 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 messages received from any other PLMN.

Table of MAPsec operation components:

- The security policy database (SPD) shall contain a table of MAPsec operation components for incoming messages. This table contains operation components which have to be carried in MAPsec messages with Protection Mode 1 or 2. The use of MAPsec operation components is specified in Annex B.

Uniformity of protection profiles:

- In order to ensure full protection, a particular PLMN shall use the same protection profile for incoming MAPsec messages from all other PLMNs. In particular, full protection is not ensured when protection profile A (no protection) is used for some source PLMNs and other profiles are used for other source PLMNs.

Explicit policy configuration:

- The SPD shall contain an entry for each PLMN the MAP-NE is allowed to communicate with.

Editor's note: Some issues need to be investigated: Non-synchronised expiration times issue, mechanism to distinguish inbound/outbound SPDs ?