3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010124**

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** ⌘ rev **1** ⌘ 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:	⌘	Clarifications in SPD and SAD contents
Source:	⌘	SA WG3 (MAP ad-hoc)
Work item code:	⌘	SEC1-MAP ***Date:*** ⌘ September 13, 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:	⌘	Solution to problems on Policy of SA renewal and START time in editors note in 5.3
Summary of change:	⌘	Clarification of informative procedures to renew SAs
Consequences if not approved:	⌘	Specification remains incomplete.

Clauses affected:	⌘	5.3, A.1
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.

Editor's note: Some issues need to be investigated: Include and clarify fallback indicator; ~~Policy for SA renewal, the need for START time~~ Non-synchronised expiration times issue, 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).

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.

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. 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 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.~~