CR-Form-v4

CHANGE REQUEST

| ⌘ | **33.200** CR **004** | ⌘ | 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: ⌘	Informative annex for overview of message MAPsec processing	
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: ⌘	Add clarification on how a MAP message is processed when applying MAPsec
Summary of change: ⌘	High level description of the processing of MAP messages in MAPsec
Consequences if not approved: ⌘	Implementors may find it more difficult to determine how to process MAP messages in the context of MAPsec

Clauses affected: ⌘	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.

Annex B (informative): Guidelines for MAP message processing

This informative annex gives high-level guidelines on the procedures a MAPsec-enabled NE must follow when processing a MAP message to be sent to or that has been received from a peer NE located in another PLMN. There is no requirement to precisely follow the procedures described below but the external effect should be equivalent.

B.1 Outgoing MAP message

When a MAPsec-enabled NE must send a MAP message to a peer NE in another PLMN, it first retrieves the security policy corresponding to that remote PLMN (ie. Looking for an entry in the SPD that matches the PLMN identifier). If no entry is found for that PLMN, it means that no MAPsec protection is required for that PLMN.

If an entry is found but does not point to any valid MAPsec SA, this is an error condition and appropriate actions must be taken by the NE (such as reporting the error to a management station). The MAP message must consequently not be further processed and should be discarded.

If an entry is found and points to one or more valid MAPsec SAs, the NE chooses the one expiring the sooner and applies this MAPsec SA to the MAP message. Once this is done, the MAP message can be sent.

B.2 Incoming MAP message

When a MAPsec-enabled NE receives a MAPsec message from a peer NE in another PLMN, it uses the fields (PLMN-id, Security Parameter Index) in the MAPsec header to find the appropriate MAPsec SA in the SAD. If none is found, the message should be rejected and the management system should be notified in some way about this event.

If the MAPsec SA is found in the SAD, then the information elements associated to that SA are used to process the MAP message. If this is successful, the message is further normally processed; otherwise, the message should be rejected and the management system should be notified in some way about this event.

The NE must also check in the inbound SDB whether the MAPsec SA used to protect the MAP message is indeed a valid MAPsec SA for the peer PLMN, in terms of policy. If the MAPsec SA is not an SA referred to by the SPD entry for that remote PLMN, then the message should be rejected and the management system should be notified in some way about this event.