3GPP TSG-SA WG3 Meeting #20 ***Tdoc S3-010467***
Sydney, Australia, 16-19. October 2001

CR-Form-v4

CHANGE REQUEST

⌘ **33.200** **CR** **CRNum** ⌘ 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 **X**

Title:	⌘	The Soft Lifetime for the MAPsec SA
Source:	⌘	Nokia
Work item code:	⌘	MAPsec
Date:	⌘	5-10-2001
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 MAPsec SA of the receiver can expire before it receives all transmitted packets if the hard lifetime is only used. Duration of communication failure depends on difference of UTC time between communicating network elements and transmission delay.
Summary of change:	⌘	To avoid the problem of stalling communication between network elements, a replacement SA is taken in use before the existing SA expires. Soft lifetime is used to warn the implementation to change SA for the outbound traffic.
Consequences if not approved:	⌘	A communication failure during the SA replacement.

Clauses affected:	⌘	3.1, 5.2, 5.4, Annex A.1and 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.

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Anti-replay protection: Anti-replay protection is a special case of integrity protection. Its main service is to protect against replay of self-contained packets that already have a cryptographical integrity mechanism in place.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

Security Association: A logical connection created for security purposes. All traffic traversing a security association is provided the same security protection. The security association specifies protection levels, algorithms to be used, lifetimes of the connection etc.

MAPsec: The complete collection of protocols and procedures needed to protect MAP messages. MAPsec can be divided into three main parts. These are (1) MAPsec transport security, (2) MAPsec Local Security Association distribution and (3) MAPsec Inter-domain Security Association and Key Management procedures.

5.2 Properties and tasks of MAPsec enabled network elements

MAPsec MAP-NEs shall maintain the following databases:

- NE-SPD-MAP: A database in an NE containing MAP security policy information (see clause 5.3);
- NE-SADB-MAP: A database in an NE containing MAP-SA information. MAP-NEs shall monitor the SA hard lifetime and expired SAs shall be deleted from the database (see clause 5.4).

MAPsec MAP-NEs shall be able to perform the following operations:

- Secure MAP signalling (i.e. send/receive protected or unprotected messages) according to information in NE-SPD-MAP and NE-SADB-MAP. The structure of protected messages is defined in clause 5.5 and the protection algorithms are defined in clause 5.6.

5.4 MAPsec security association attribute definition

The MAPsec security association shall contain the following data elements:

- **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.

- **SA Hard Lifetime:**

  Defines the actual expiry time of the SA. The ~~expiry of the~~ hard lifetime shall be given in UTC time.

- **SA Soft Lifetime:**

  Defines soft expiry time of the SA for outbound traffic. The soft lifetime shall be given in UTC time. Soft lifetime ≤ hard lifetime.

Editor's Note: The exact format and length to be defined.

When the soft lifetime is reached, a replacement SA shall be used for the outbound traffic. The current SA shall be used if an appropriate replacement SA does not exist.

A MAPsec SA is uniquely identified by a destination PLMN-Id and a Security Parameters Index, SPI. As a consequence, during SA creation, the SPI is always chosen by the receiving side.

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

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 how to carry out the initial exchange of MAPsec SAs;
- to define 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~~ hard lifetime 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~~ soft lifetime is reached, unless the replacement SA does not exist or 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 soft lifetimes and hard lifetimes (expiry times).

Annex B (normative): MAPsec message flows

Imagine a network scenario with two MAP-NEs at different PLMNs (NEa and NEb) willing to communicate using MAPsec. Figure 1 presents the message flow.

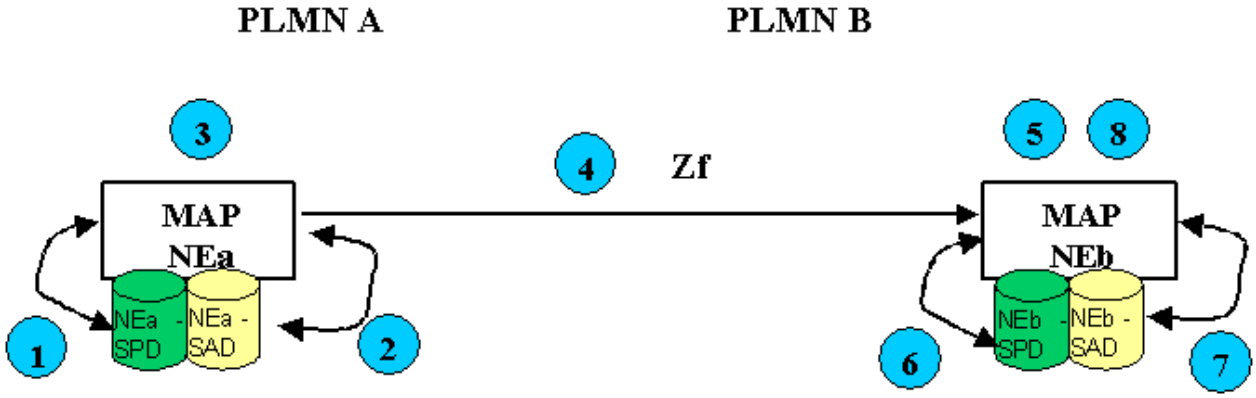

Figure 1. MAPsec Message Flow

According to Figure 1, when MAP-NEa (NEa) from PLMN A wishes to communicate with a MAP-NEb (NEb) of PLMN B using MAP protocol, the process is the following:

As the Sending Entity, NEa performs the following actions during the outbound processing of every MAP message:

1. NEa checks its Security Policy Database (SPD) to check if MAP security mechanisms shall be applied towards PLMN B:

   a) If the SPD does not mandate the use of MAPsec towards PLMN B, then normal MAP communication procedures will be used and the process continues in step 4.b.

   b) If the SPD mandates the use of MAPsec towards PLMN B, then the process continues at step 2.

   c) If no valid entry in the SPD is found for PLMN B, then the communication is aborted and an error is returned to.

2. NEa checks its Security Association Database (SAD) for a valid Security Association (SA) to be used towards PLMN B. In the case where more than one valid SA is available at the SAD, NEa shall choose the one ~~expiring the~~, which soft lifetime is reached sooner.

   a) In case protection of MAP messages towards PLMN B is not possible (e.g. no SA available, invalid SA…), then the communication is aborted and an error is returned to MAP user.

   b) If a valid SA exists but the MAP dialogue being handled does not require protection (Protection Mode 0 applies to all the components of the dialogue), then either the original MAP message in cleartext is sent in step 4.b, or a MAPsec message with Protection Mode 0 is created in step 3.

   c) If a valid SA exists and the MAP dialogue being handled requires protection, then the process continues at step 3.