Technical Specification Group Services and System Aspects
Meeting #14, Kyoto, Japan, 17-20 December 2001

TSGS#14(01)0618

Source: **SA WG3**

Title: **2 CRs to 33.200: MAPsec SA related (Rel-4)**

Document for: **Approval**

Agenda Item: **7.3.3**

Spec	CR	Rev	Phase	Cat	Subject	Version-Current	Version-New	Doc-2nd-Level
33.200	016		Rel-4	F	The Soft Expiry Time for the MAPsec SA	4.1.0	4.2.0	S3-010560
33.200	019		Rel-4	F	Completing the specification of a MAPsec SA	4.1.0	4.2.0	S3-010693

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

Tdoc S3-010560

CR-Form-v4

CHANGE REQUEST

⌘ **33.200 CR 016** ⌘ 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:	⌘	The Soft Expiry Time for the MAPsec SA		
Source:	⌘	SA WG3		
Work item code:	⌘	SEC1-MAP	***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 expiry time 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 expiry time 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:	⌘		

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 expiry ~~life~~time 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 Expiry Time~~Lifetime~~:**

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

- **SA Soft Expiry Time:**

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

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

After the hard expiry time has been reached the SA shall no longer be used for inbound or outbound traffic. When the soft expiry time is reached, the SA shall not be used any longer for the outbound traffic unless no other valid SA exists.

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 expiry times~~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.~~

An SA being used by an NE for incoming traffic expires when it reaches its hard expiry time. When this occurs, the NE can no longer use that SA to process incoming MAPsec traffic. If a new additional valid SA is installed into the NE, the "old" one must still be kept by the NE until it reaches its hard expiry time, so as to be able to accept incoming traffic still received under the "old" SA.

~~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.~~

An SA being used by an NE for outgoing traffic expires when it reaches its soft expiry time. When this occurs, the NE must start using another valid SA. If no such valid SA exists, the NE continues to use the "old" SA until it reaches its hard expiry time or another valid SA effectively becomes available.

In case the current SA gets compromised, a new valid SA should be made immediately available to the NE, which should then stop using the compromised SA and delete it.

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 and hard expiry times.

When more than one valid SA is available, the NE chooses the one for which the soft expiry time will be reached next.

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.

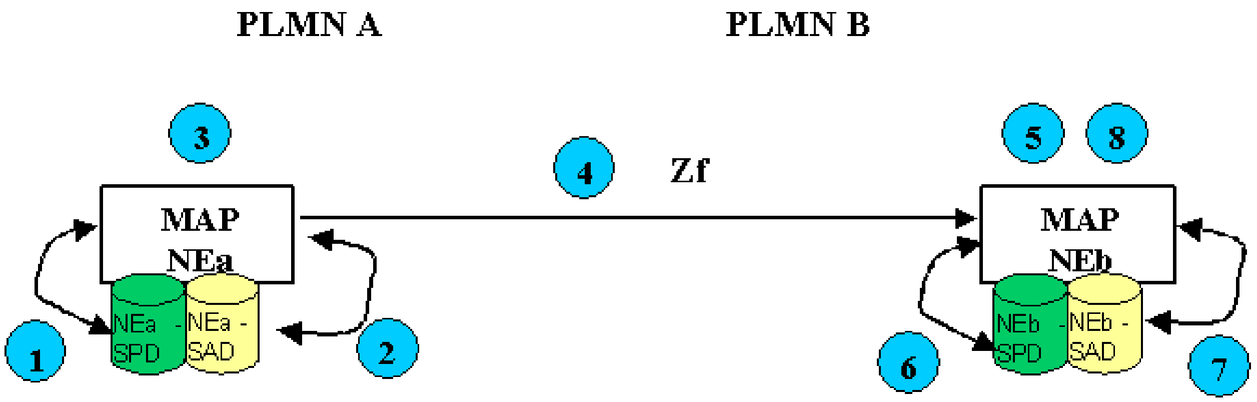

Figure 1. MAPsec Message Flow

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, the soft expiry time of which will be reached next. ~~expiring the 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.

3. NEa constructs the MAPsec message towards NEb using the parameters (keys, algorithms and protection profiles) found in the SA.

4. NEa generates either:

   a) MAPsec message towards NEb.

   b) An unprotected MAP message in the event that the SPD towards NEb or protection profiles for that specific MAP dialogue so allows it (1.a. or 2.b.).

At the Receiving Entity, NEb performs the following actions during the inbound processing of every MAP message it received:

5. If an unprotected MAP message is received, the process continues with step 6.

   Otherwise, NEb decomposes the received MAPsec message and retrieves basic information to apply security measures (‘SPI’, ‘sending PLMN-ID’, ‘TVP’, ‘IV’ and ‘Original Component Identifier’).

   Freshness of the protected message is checked at this time. If the Time Variant Parameter (TVP) received in the protected message is out of the acceptable window then the message shall be discarded and an error is returned to MAP user. No error message is returned to NEa.

6. NEb checks the SPD:

   An unprotected MAP message is received:

   a) If an unprotected MAP message is received and fallback to unprotected mode is allowed, then the unprotected MAP message is simply processed (Process goes to END)

   b) If an unprotected MAP message is received and the ‘MAPsec operation components table’ of the SPD does not mandate the use of MAPsec for the included ‘Original Component Identifier’, then the unprotected MAP message is simply processed (Process goes to END)

   c) If an unprotected MAP message is received, the ‘MAPsec operation components table’ of the SPD mandates the use of MAPsec for the included ‘Original Component Identifier’ and fallback to unprotected mode is NOT allowed, then the message is discarded.

   If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

   A MAPsec message is received:

   d) If no valid entry in the SPD is found for PLMN A, then the message is discarded and an error is reported to MAP user.

      If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

   e) If a MAPsec message is received, but the SPD indicates that MAPsec is NOT to be used, then the message is discarded and an error is reported to MAP user.

      If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

   f) If a MAPsec message is received and the SPD indicates that MAPsec is required, then the process continues at step 7.

7. NEb checks its SAD to retrieve the relevant SA-information for processing of the MAPsec message:

   a) If the received SPI points to a valid SA, then the process continues at step 8.

   b) If the received SPI does not point to a valid SA, the message is discarded and an error is reported to MAP user. If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

8. Integrity and encryption mechanisms are applied on the message using the information in the SA (Keys, algorithms, protection profiles).

   a) If the result after applying such mechanisms is NOT successful then the message is discarded and an error is reported to MAP user. If the MAP dialogue is still open and it is waiting for an answer, NEb also reports an error back to NEa.

   b) If the result after applying such procedures is successful, then NEb has the cleartext MAP message NEa originally wanted to send NEb. The cleartext MAP message can now be processed (Process goes to END)

END: A cleartext MAP message is available at NEb.

In the event the received message at NEb requires an answer to NEa (Return Result/Error), NEb will perform the process in steps 1 to 4 acting as the Sender and NEa will perform the process in steps 5 to 8 acting as the Receiver.

In the event a MAPsec enabled NE initiated a secured MAP communication towards a non-MAPsec enabled NE and the MAPsec enabled NE received an error indication of such circumstance (i.e. "ApplicationContextNotSupported"). The MAPsec enabled NE shall check whether "Fallback to Unprotected Mode" is allowed:

- If NOT allowed, then the communication is aborted.
- If allowed, then the MAPsec enabled NE shall send an unprotected MAP message instead.

The same procedures shall apply to secure MAP communications between MAP-NEs in the same PLMN.

NOTE: Because various error cases may be caused by active attacks, it is highly recommended that the cases are reported to the management system.

3GPP TSG SA WG3 Security — S3#20 **S3-010693**
27 - 30 November, 2001
Sophia Antipolis, France

CR-Form-v4

CHANGE REQUEST

⌘ **33.200 CR 019** ⌘ 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:	⌘	Completing the specification of a MAPsec SA		
Source:	⌘	SA WG3		
Work item code:	⌘	SEC1-MAP	***Date:*** ⌘	22-11-01
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:	⌘	To explicitly complete the specification of a MAPsec SA and make it clear that since destination PLMN-Id and SPI uniquely determine an SA, they should belong to that SA.
Summary of change:	⌘	Adding Destination PLMN-Id, SPI and Sending PLMN-Id to an SA.
Consequences if not approved:	⌘	The specification of an SA will be incomplete and it will be left unclear if the elements that uniquely determine an SA actually belong to that SA. The change ensures SAs can be **uniquely identified** in the SAD and avoids the possibility of incompatible implementations.

Clauses affected:	⌘	5.4		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘			

5.4 MAPsec security association attribute definition

The MAPsec security association shall contain the following data elements:

- **Destination PLMN-Id:**

  PLMN-Id is the ID number of the receiving Public Land Mobile Network (PLMN). The value for the PLMN-Id is a concatenation of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the receiving network.

- **Security Parameters Index (SPI):**

  SPI is a 32-bit value that is used in combination with Destination PLMN-Id to uniquely identify a MAP-SA.

- **Sending PLMN-Id:**

  PLMN-Id is the ID number of the sending Public Land Mobile Network (PLMN). The value for the PLMN-Id is a concatenation of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the sending network.

- **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 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 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.