ETSI TS 133 200 V6.1.0 (2005-03)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
3G Security;
Network Domain Security (NDS);
Mobile Application Part (MAP) application layer security
(3GPP TS 33.200 version 6.1.0 Release 6)

Reference

RTS/TSGS-0333200v610

Keywords

UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The absence of security in Signalling System No. 7 (SS7) networks is an identified security weakness in 2G systems. This was formerly perceived not to be a problem, since the SS7 networks were the provinces of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions.

For 3G systems it is a clear goal to be able to protect the core network signalling protocols, and by implication this means that security solutions must be found for both SS7 and IP based protocols.

Various protocols and interfaces are used for control plane signalling within and between core networks. The security services that have been identified as necessary are confidentiality, integrity, authentication and anti-replay protection. These will be ensured by standard procedures, based on cryptographic techniques.

1 Scope

This technical specification covers the security mechanisms and procedures necessary to protect the MAP protocol. The complete set of enhancements and extensions to facilitate security protection for the MAP protocol is termed MAPsec and it covers transport security in the MAP protocol itself and the security management procedures.

The security mechanisms specified for MAP are on the application layer. This means that MAPsec is independent of the network and transport protocols to be used.

This technical specification contains the stage-2 specification for security protection of the MAP protocol. The actual implementation (stage-3) specification can be found in the MAP stage-3 specification, TS 29.002 [4].

NOTE: It is explicitly noted that automated key management and key distribution is not part of Rel-5. All key management and key distribution in Rel-5 shall therefore be carried out by other means (see Annex A).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3G TS 21.133: Security Threats and Requirements.

[2] 3G TS 21.905: 3G Vocabulary.

[3] 3G TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2.

[4] 3G TS 29.002: Mobile Application Part (MAP) specification.

[5] NIST Special Publication 800-38A "Recommendation for Block Cipher Modes of Operation" December 2001.

[6] ISO/IEC 9797: "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher", Ed.1, 1999-12-16.

[7] FIPS Publication 197: "Specification for the Advanced Encryption Standard (AES)", November 26, 2001.

3 Definitions, symbols and abbreviations

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.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

f6	MAP encryption algorithm.
f7	MAP integrity algorithm.
Zf	The MAP application layer security interface between MAP-NEs engaged in security protected signalling.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
FALLBACK	Fallback to unprotected mode indicator
IP	Internet Protocol
IV	Initialisation Vector
MAC	Message Authentication Code
MAC-M	MAC used for MAP
MAP	Mobile Application Part
MAP-NE	MAP Network Element
MAPsec	MAP security – the MAP security protocol suite
MEA	MAP Encryption Algorithm identifier
MEK	MAP Encryption Key
MIA	MAP Integrity Algorithm identifier
MIK	MAP Integrity Key
NDS	Network Domain Security
NE	Network Entity
PPI	Protection Profile Indicator
PPRI	Protection Profile Revision Identifier
PROP	Proprietary field
SA	Security Association
SADB	Security Association DataBase (also referred to as SAD)
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
TVP	Time Variant Parameter

3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

4 Principles of MAP application layer security

This technical specification defines mechanisms for protecting the MAP protocol at the application layer. The MAP protocol may also be protected at the network layer when IP is used as the transport protocol. However, whenever inter-working with networks using SS7-based transport is necessary, protection at the application layer shall be used.

The security measures specified in this TS are only fully useful if all interconnected operators use them. In order to prevent active attacks all interconnected operators must at least use MAPsec with the suitable protection levels as indicated in this specification and treat the reception of all MAP messages (protected and unprotected) in a uniform way in the receiving direction.

Before protection can be applied, Security Associations (SA) needs to be established between the respective MAP network elements. Security associations define, among other things, which keys, algorithms, and protection profiles to use to protect MAP signalling. The necessary MAPsec-SAs between networks are negotiated between the respective network operators. The negotiated SA will be effective PLMN-wide and distributed to all network elements which implement MAP application layer security within the PLMN. Signalling traffic protected at the application layer will, for routing purposes, be indistinguishable from unprotected traffic to all parties except for the sending and receiving entities.

Protection at the application layer implies changes to the application protocol itself to allow for the necessary security functionality to be added.

The interface applies to all MAPsec transactions, intra- or inter-PLMN.

Annex B includes detailed procedures on how secure MAP signalling is performed between two MAP-NEs.

NOTE: A limited level of MAP message authenticity can be achieved without the use of MAPsec by using a TCAP handshake prior to the MAP payload exchange. Annex C describes the use of the TCAP handshake for MAP SMS transfers.

5 MAP security (MAPsec)

5.1 Security services provided by MAPsec

The security services provided by MAPsec are:

- data integrity;
- data origin authentication;
- anti-replay protection;
- confidentiality (optional).

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 MAPsec-SA information. MAP-NEs shall monitor the SA hard expiry 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.

5.3 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 NEs 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 ?

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 MAPsec-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 Revision Identifier (PPRI):**

  Contains the revision number of the PPI. Length is 8 bits. PPRI-values are defined in section 6.3.

- **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:**

  Defines the actual expiry time of the SA. The hard expiry 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.

5.5 MAPsec structure of protected messages

MAPsec provides for three different protection modes and these are defined as follows:

Protection Mode 0: No Protection

Protection Mode 1: Integrity, Authenticity

Protection Mode 2: Confidentiality, Integrity, and Authenticity

MAP operations protected by means of MAPsec consist of a Security Header and the Protected Payload. Secured MAP messages have the following structure:

Security Header	Protected Payload

In all three protection modes, the security header is transmitted in cleartext.

In protection mode 2 providing confidentiality, the protected payload is essentially the encrypted payload of the original MAP message. For integrity and authenticity in protection mode 1, the message authentication code is calculated on the security header and the payload of the original MAP message in cleartext and it is included in the protected payload. The message authentication code in protection mode 2 is calculated on the security header and the encrypted payload of the original MAP message. In protection mode 0 no protection is offered, therefore the protected payload is identical to the payload of the original MAP message.

5.5.1 MAPsec security header

For Protection Mode 0, the security header is a sequence of the following data elements:

Security header = SPI || Original component Id

For Protection Modes 1 and 2, the security header is a sequence of the following elements:

Security header = SPI || Original component Id || TVP || NE-Id || Prop

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

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

- **Original component Id:**

  Identifies the type of component (invoke, result or error) within the MAP operation that is being securely transported (Operation identified by operation code, Error defined by Error Code or User Information).

- **TVP:**

  The TVP is used for replay protection of Secured MAP operations is a 32 bit time-stamp. The receiving network entity will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived is 0.1 seconds. The size of the time-window at the receiving network entity is not standardised.

- **NE-Id:**

  6 octets used to create different IV values for different NEs within the same TVP period. It is necessary and sufficient that *NE-Id* is unique per PLMN. (This is sufficient because sending keys are unique per PLMN.) The NE-Id shall be the E.164 global title of the NE without the MCC and MNC.

- **Proprietary field (PROP):**

  4 octets used to create different IV values for different protected MAP messages within the same TVP period for one NE. The usage of the proprietary field is not standardised.

5.5.2 Protected payload

5.5.2.1 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the protected payload of Secured MAP messages in protection mode 0 is identical to the original MAP message payload in cleartext.

5.5.2.2 Protection Mode 1

The protected payload of Secured MAP messages in protection mode 1 takes the following form:

Cleartext|| f7(Security Header||Cleartext)

where "Cleartext" is the payload of the original MAP message in cleartext. Therefore, in Protection Mode 1 the protected payload is a concatenation of the following information elements:

- Cleartext
- Message authentication code (MAC-M) calculated by the function f7

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC-M) function f7 with the integrity key defined by the security association to the concatenation of Security Header and Cleartext. The MAC-M length shall be 32 bits.

5.5.2.3 Protection Mode 2

The protected payload of Secured MAP Messages in protection mode 2 takes the following form:

f6(Cleartext) || f7(Security Header|| f6(Cleartext))

where "Cleartext" is the original MAP message payload in cleartext. Confidentiality is achieved by encrypting Cleartext using the encryption function f6 with the confidentiality key defined by the security association and the initialisation vector (IV). Authentication of origin and integrity are achieved by applying the message authentication code (MAC-M) function f7 with the integrity key defined by the security association to the concatenation of Security Header and ciphertext. The MAC-M length shall be 32 bits. The length of the ciphertext is the same as the length of the cleartext.

5.6 MAPsec algorithms

5.6.1 Mapping of MAPsec-SA encryption algorithm identifiers

The MEA algorithm indication fields in the MAPsec-SA are used to identify the encryption algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below.

Table 1: MAP encryption algorithm identifiers

MAP Encryption Algorithm identifier	Description
0	Null
1	AES in counter mode with 128-bit key length (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.1.1 Description of MEA-1

The MEA-1 algorithm is AES [7] used in counter mode with a 128-bit key and 128-bit counter blocks as described in clause 6.5 of FIPS 800-38A Recommendation for Block Cipher Modes of Operation [5]. The initial counter block T_1 is initialized with IV. Successive counter blocks T_j (J>1) are derived by applying an incrementing function over the entire block T_{j-1} (J>=2) (see Appendix B.1: The standard incrementing function of [5]).

5.6.2 Mapping of MAPsec-SA integrity algorithm identifiers

The MIA algorithm indication fields in the MAPsec-SA are used to identify the integrity algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below.

Table 2: MAP integrity algorithm identifiers

MAP Integrity Algorithm identifier	Description
0	Null
1	AES in a CBC MAC mode with a 128-bit key (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.2.1 Description of MIA-1

The MIA-1 algorithm is the ISO/IEC 9797 Part 1: padding method 2, MAC algorithm 1 (initial transformation=1, output transformation=1). No IV used. The MAC-length m is 32-bits (see clause 5.6.1). See ISO/IEC 9797 [6] for more information.

5.6.3 Construction of IV

The IV used in the encryption shall be constructed as follows:

$$IV = TVP \,||\, NE\text{-}Id \,||\, Prop \,||\, Pad$$

The padding field is used to expand *TVP* || *NE-Id* || *Prop* to the *IV* length required by the cryptographic scheme in use.

The IV length shall be 16 octets. The padding (Pad) shall be 2 octets with all bits set to zero.

6 MAPsec protection profiles

6.1 Granularity of protection

MAPsec protection is specified per MAP operation component.

6.2 MAPsec protection groups

This section specifies groups of messages and their protection modes at the operation component level. Individual protection groups or particular combinations of groups can then be used to construct protection profiles as specified in section 6.3.

Combinations of overlapping protection groups are forbidden. Forbidden combinations are explicitly specified in 6.2.1 below.

The concept of "protection levels" is introduced to administrate the protection mode on operation component level. A protection level of an operation determines the protection modes used for the operation's components according to the following table.

Table 3: MAPsec protection levels

Protection level	Protection mode for *invoke* component	Protection mode for *result* component	Protection mode for *error* component
1	1	0	0
2	1	1	0
3	1	2	0
4	2	1	0
5	2	2	0
6	2	0	0

6.2.1 MAPsec protection groups

6.2.1.1 MAP-PG(0) – No Protection

This MAP-PP does not contain any operation and it does not protect any information. It is useful however to have a "null" MAP-PP to use in situations where no security is required or is an option. This protection group cannot be combined with any other protection group.

6.2.1.2 MAP-PG(1) – Protection for Reset

Table 4: PG(1) – Protection for Reset

Application Context/Operation	Protection Level
ResetContext-v2/ Reset	1
ResetContext-v1/ Reset	1

6.2.1.3 MAP-PG(2) – Protection for Authentication Information except Handover Situations

Table 5: PG(2) – Protection for Authentication Information except Handover Situations

Application Context/Operation	Protection Level
InfoRetrievalContext-v3/ Send Authentication Info	3
InfoRetrievalContext-v2/ Send Authentication Info	3
InfoRetrievalContext-v1/ Send Parameters	3
InterVlrInfoRetrievalContext-v3/ Send Identification	3
InterVlrInfoRetrievalContext-v2/ Send Identification	3

6.2.1.4 MAP-PG(3) – Protection for Authentication Information in Handover Situations

Table 6: PG(3) – Protection for Authentication Information in Handover Situations

Application Context/Operation	Protection Level (Component level)
HandoverControlContext-v3/ Prepare Handover (Note that the AC contains also other operations)	4
HandoverControlContext-v3/ Forward Access Signalling (Note that the AC contains also other operations)	4
HandoverControlContext-v2/ Prepare Handover (Note that the AC contains also other operations)	4
HandoverControlContext-v2/ Forward Access Signalling (Note that the AC contains also other operations)	4
HandoverControlContext-v1/ Perform Handover (Note that the AC contains also other operations)	4
HandoverControlContext-v1/ Forward Access Signalling (Note that the AC contains also other operations)	4

6.2.1.5 MAP-PG(4) – Protection of non location dependant HLR data

Table 7: PG(4) – Protection of non location dependant HLR data

Application Context/Operation	Protection Level
AnyTimeInfoHandlingContext-v3 / AnyTimeModification	1

6.3 MAPsec protection profiles

Protection profiles can be individual protection groups or particular combinations of protection groups. MAP protection profiles are coded as a 16 bit binary number where each bit corresponds to a protection group. The protection that shall be applied to a MAPsec message is uniquely identified by the combination of PPRI and PPI.

This specification contains the MAPsec protection profiles that are identified with PPRI having value 0. Currently only 5 groups are defined, the rest are reserved for future use.

Table 8: Protection profile encoding

Protection profile bit	Protection group
0	No protection
1	Reset
2	Authentication information except handover situations
3	Authentication information in handover situations
4	Non-location dependant HLR data
5-15	Reserved

Protection profiles shall be bidirectional.

The following protection profiles are defined.

Table 9: Protection profile definition

Protection profile name	**Protection group**				
	PG(0) *No protection*	PG(1) *Reset*	PG(2) *AuthInfo except handover situations*	PG(3) *AuthInfo in handover situation*	PG(4) *Non-location dependant HLR data*
Profile A	✓				
Profile B		✓	✓		
Profile C		✓	✓	✓	
Profile D		✓	✓	✓	✓
Profile E		✓	✓		✓

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 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, etc (MAPsec SAs are expected to be fairly long lived).

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.

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. 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.

A.2 Local Security Association Distribution

Manual Local Security Association Distribution is executed entirely within one PLMN and is consequently at the discretion of the administrative authority.

The requirement on the manual distribution procedures can be summarized as follows:

- Procedures for transporting the relevant MAPsec SA to the MAP-NEs must be defined. In order to ensure that the MAPsec SA are present when needed, all valid MAPsec SA should be distributed to all MAP-NEs as soon as they are available.
- Procedures for revocation of MAPsec SAs must be defined.

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.

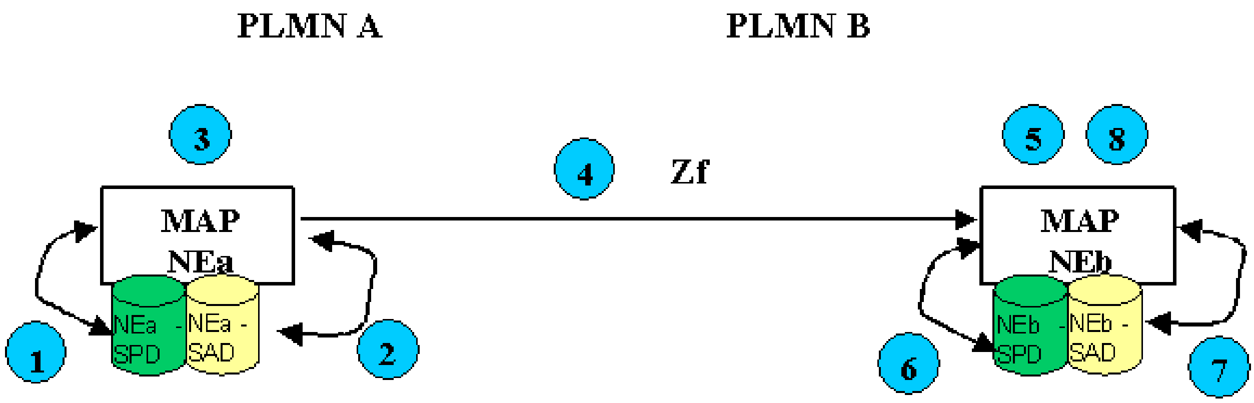

Figure 1. MAPsec Message Flow

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 the MAP user.

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.

    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 SPI and Original component Id from the security header.

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, NEb checks SPI in the SPD:

   d) If SPI is not in SPD or there is no valid entry for the PLMN associated with SPI in the SPD, 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 NEb uses the "Original Component Identifier" in the MAPsec header to identify the protection level that has to be applied to the component indicated, according to the protection profile indicated in the SA. If Protection Mode 0 was applied, then the MAP message is simply processed (Process goes to END). Otherwise 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. Freshness of the protected message is checked by ensuring the Time Variant Parameter (TVP) is in an acceptable window. Integrity and encryption mechanisms are applied to the message according to the identified protection level, by using the information in the SA (Keys, algorithms).

   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.

Annex C (normative): Using TCAP handshake for SMS transfer

The SMS Gateway/Interworking MSC operator and the serving node (MSC or SGSN) operator may agree to use the TCAP handshake as a countermeasure against SMS fraud for messages exchanged between their networks (for detailed message flows see TS 29.002 [4]). A limited level of authenticity is provided by the following mechanisms.

C.1 Mobile Terminated SMS

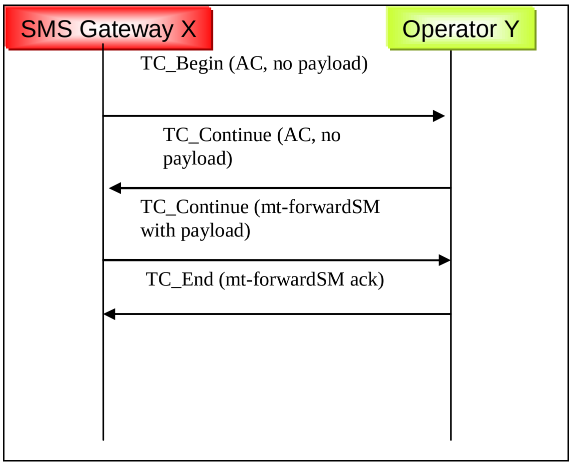

Figure C.1: MAP mt-Forward-SM messages using a TCAP Handshakes

If the serving network receives an mt-forward-SM MAP message which uses the TC_Continue to transfer the MAP payload then it is guaranteed that the SCCP calling party address of the (empty) TC_Begin message is authentic, otherwise the first TC-continue message would be sent to the falsified address. The correct message flow is guaranteed by the TCAP transaction capabilities (use of Transaction ID).

Unfortunately there are some ways in which a fraudulent SMS Gateway operator (called the originator in bullets (a) and (b)) may try to circumvent the implicit SCCP address authentication provided by the TCAP handshake.

(a) The originator includes a falsified SMS-GMSC address as SM-RP-OA in the mt-forward-SM payload carried by the TC-continue (third message in figure C.1)

(b) The originator tries to predict the TCAP transaction ID assigned by the serving node, which is to be used within the third message, and spoofs the third message without waiting for the second message. This attack has to be carried out within the right time window.

If TCAP handshake is to be used, the following measure shall be taken within the network of the serving node in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator.

MEAS-1: The receiving network shall verify if the received SMS-GMSC address (as SM-RP-OA in the third message) may be used from the SCCP Calling Party Address. Some operators use a single SMS-GMSC address for a range of SCCP Calling Party Addresses and this will need to be taken into consideration.

If TCAP handshake is to be used, at least one of the following measures shall be taken within the network of the serving node in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator.

MEAS-2a: The receiving node shall use mechanisms to ensure that the destination TCAP transaction ID which needs to be used within the third message is predictable with a probability of less than $1 / 2^{10}$ for a third party knowing all previous TCAP transaction ID values.

MEAS-2b: The receiving network shall wait n seconds before it processes the third message (TC-continue(mt-forwardSM with payload)). This should ensure that the TC_abort from the spoofed network is processed at the destination node earlier than a TC_continue including a successfully guessed TCAP Transaction ID value.

The following grouping method may be used for an operator to gradually introduce the TCAP handshake for mt-Forward-SM messages. Define an "operator group-1" as a trusted operator group and "operator group-2" as an un-trusted operator group. Agree that group-1 uses the TCAP handshake, while group-2 does not use the TCAP handshake. As specified by TS 29.002 [4] this requires that the SMS Gateway operators belonging to group-1 shall either use application context2 or 3 for mt-Forward-SM. The management of the two groups requires that the serving network shall implement a policy table of SCCP Calling Party Addresses for which a TCAP handshake is required.

If the above described grouping method is used then the following measure shall be taken at the serving network in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator that tries to circumvent the policy table checks.

MEAS-3: The serving network shall verify that the SCCP Calling Party Address of a first message with a payload (i.e. not using the TCAP handshake) is not from an SMS-GMSC-address as SM-RP-OA that shall use the TCAP handshake.

The benefit gained for operators that belong to group-1 is that spoofing of their SMS-GMSC-addresses is practically difficult if the policy table has been administrated accurately.

C.2 Mobile Originated SMS

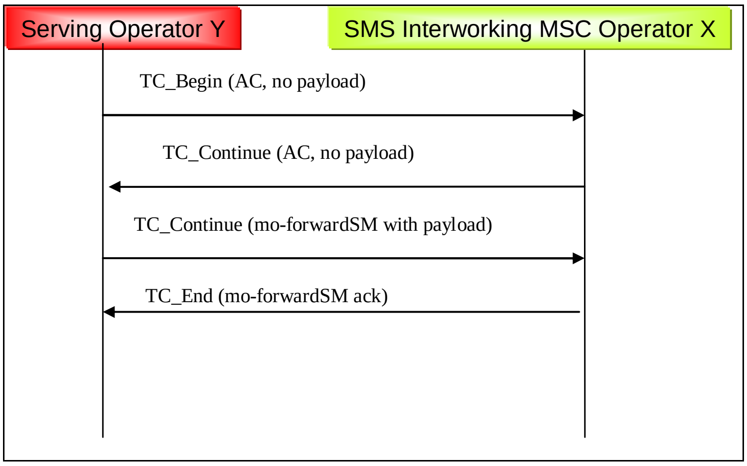

Figure C.2: MAP mo-Forward-SM messages using a TCAP Handshakes

If the serving network sends an mo-forward-SM MAP message which uses the TC_Continue to transfer the MAP payload then it is guaranteed that the SCCP calling party address of the (empty) TC_Begin message is authentic, otherwise the first TC-continue message would be sent to the falsified address. The correct message flow is guaranteed by the TCAP transaction capabilities (use of Transaction ID).

Unfortunately there are some ways in which a fraudulent serving (MSC or SGSN) operator (called the originator in bullets (a) and (b)) may try to circumvent the implicit SCCP address authentication provided by the TCAP handshake.

(a) The originator includes a falsified MSISDN as SM-RP-OA within the mo-forward-SM payload carried by the TC-continue (third message in figure C.2)

(b) The originator tries to predict the TCAP transaction ID assigned by the serving node, which is to be used within the third message, and spoofs the third message without waiting for the second message. This attack has to be carried out within the right time window.

If TCAP handshake is to be used, the following measure may be taken within the network of the SMS Interworking MSC in order to counteract the spoofing possibilities of a malicious mo-Forward-SM originator.

MEAS-1: The receiving node (i.e. SMS interworking MSC) may query the HLR to verify if the received SCCP Calling Party Address of the mo-forward-SM is from the same network which is currently serving the subscriber (MSISDN contained in SM-RP-OA in the third message).

If the TCAP handshake is to be used, then at least one of MEAS-2a and MEAS-2b of clause C.1 shall also be applied.

The following grouping method may be used for an operator to gradually introduce the TCAP handshake for mo-Forward-SM messages. Define an 'operator group-1' as a trusted operator group and 'operator group-2' as an un-trusted operator group. Agree that group-1 uses the TCAP handshake, while group-2 does not use the TCAP handshake. As specified by TS 29.002 [4] this requires that the MSC operators belonging to group-1 shall either use application context2 or 3 for mo-Forward-SM. The management of the two groups requires that the network of the SMS Interworking MSC shall implement a policy table of originating SCCP-addresses for which a TCAP handshake is required.

If the above described grouping method is used then the following measure shall be taken at the network of the SMS Interworking MSC in order to counteract the spoofing possibilities of a malicious mo-Forward-SM originator that tries to circumvent the policy table checks.

MEAS-3: The SMS Interworking MSC shall verify that the SCCP Calling Party address of a first message with a payload (i.e. not using the TCAP handshake) is not from an address that shall use the TCAP handshake.

The benefit gained for operators that belong to group-1 is that mo-Forward-SM spoofing for their subscribers, while roaming within group-1, becomes practically difficult if the policy table has been administrated accurately.

Annex D (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
12-2004	SP-26	SP-040921	023	2	SMS fraud countermeasures	5.1.0	6.0.0
03-2005	SP-27	SP-050138	024	-	Correct specification of addresses used in TCAP-Handshake	6.0.0	6.1.0
03-2005	SP-27	SP-050138	025	1	Addition of TCAP-Handshake for MO-ForwardSM	6.0.0	6.1.0
03-2005	SP-27	SP-050138	026	1	Improving the robustness of the TCAP handshake mechanism	6.0.0	6.1.0

History

Document history		
V6.0.0	December 2004	Publication
V6.1.0	March 2005	Publication