

ETSI TS 133 200 V4.1.0 (2001-09)

Technical Specification

Universal Mobile Telecommunications System (UMTS); Network Domain Security - MAP (3GPP TS 33.200 version 4.1.0 Release 4)



Reference

RTS/TSGS-0333200Uv4R1

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

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, send your comment to:

editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2001.
All rights reserved.

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://www.etsi.org/legal/home.htm>).

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 www.etsi.org/key.

Contents

Intellectual Property Rights	2
Foreword.....	2
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
3 Definitions, symbols and abbreviations	5
3.1 Definitions	5
3.2 Symbols.....	6
3.3 Abbreviations	6
3.4 Conventions.....	6
4 Principles of MAP application layer security.....	7
5 MAP security (MAPsec)	7
5.1 Security services provided by MAPsec	7
5.2 Properties and tasks of MAPsec enabled network elements.....	7
5.3 Policy requirements for the MAPsec Security Policy Database (SPD)	8
5.4 MAPsec security association attribute definition	8
5.5 MAPsec structure of protected messages	9
5.5.1 MAPsec security header	9
5.5.2 Protected payload.....	10
5.5.2.1 Protection Mode 0.....	10
5.5.2.2 Protection Mode 1	10
5.5.2.3 Protection Mode 2.....	10
5.6 MAPsec algorithms	11
5.6.1 Mapping of MAP-SA encryption algorithm identifiers	11
5.6.1.1 Description of MEA-1.....	11
5.6.2 Mapping of MAP-SA integrity algorithm identifiers.....	11
5.6.2.1 Description of MIA-1.....	11
5.6.3 Construction of IV	11
6 MAPsec protection profiles.....	12
6.1 Granularity of protection	12
6.2 MAPsec protection groups	12
6.2.1 MAPsec protection groups.....	12
6.2.1.1 MAP-PG(0) – No Protection.....	12
6.2.1.2 MAP-PG(1) – Protection for Reset	12
6.2.1.3 MAP-PG(2) – Protection for Authentication Information except Handover Situations.....	13
6.2.1.4 MAP-PG(3) – Protection for Authentication Information in Handover Situations.....	13
6.2.1.5 MAP-PG(4) – Protection of non location dependant HLR data.....	13
6.3 MAPsec protection profiles	14
Annex A (informative): Guidelines for manual key management	15
A.1 Inter-domain Security Association and Key Management Procedures	15
A.2 Local Security Association Distribution	15
Annex B (normative): MAPsec message flows	16
Annex C (informative): Change history	19
History	20

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-4. All key management and key distribution in Rel-4 must 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] ISO/IEC 10116: "Information technology -- Security techniques -- Modes of operation for an n-bit block cipher", Ed.2, 1997-04-17.
- [6] ISO/IEC 9797: "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher", Ed.1, 1999-12-16.

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 cryptographic 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, lifetime 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
MEK	MAP Encryption Key
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
MIA	MAP Integrity Algorithm identifier
MIK	MAP Integrity Key
NDS	Network Domain Security
NE	Network Entity
PPI	Protection Profile Indicator
PROP	Proprietary field
SA	Security Association
SADB	Security Association DataBase
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 MAP-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 MAP application layer security interface between MAP-NEs engaged in security protected signalling is referred to in this specification as the Zf interface. 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.

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 MAP-SA information. MAP-NEs shall monitor the SA 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.

5.3 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 NE 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.

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:

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.

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

The security header is a sequence of the following data elements:

Security header = TVP // NE-Id // Prop // Sending PLMN-Id // SPI // Original component Id

- 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.

- 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.

- Security Parameters Index (SPI):

SPI is an arbitrary 32-bit value that is used in combination with the sender's PLMN-Id to uniquely identify a MAP-SA.

- Original Component identifier:

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).

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 MAP-SA encryption algorithm identifiers

The MEA algorithm indication fields in the MAP-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 a stream cipher mode (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.1.1 Description of MEA-1

The MEA-1 algorithm is the ISO/IEC 10116 Counter Mode with parameter $j=128$ bits, $SV=IV$ and truncation of the last block is according to the method described in ISO/IEC 10116 Annex A.5.3. See ISO/IEC 10116 [5] for more information.

Editor's Note: More specification on the mode of operation for MEA-1 may be required.

5.6.2 Mapping of MAP-SA integrity algorithm identifiers

The MIA algorithm indication fields in the MAP-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:

$$IV = TVP \parallel NE-Id \parallel Prop \parallel Pad$$

The padding field is used to expand $TVP \parallel NE-Id \parallel Prop$ 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 <i>invoke</i> component	Protection mode for <i>result</i> component	Protection mode for <i>error</i> 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
AnyTimInfoHandlingContext-v3 / AnyTimeModification	1
SubscriberDataMngtContext-v3 / DeleteSubscriberData	1

Editor's Note: Protection Group 4 is not complete.

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. 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) <i>No protection</i>	PG(1) <i>Reset</i>	PG(2) <i>AuthInfo except handover situations</i>	PG(3) <i>AuthInfo in handover situation</i>	PG(4) <i>Non-location dependant HLR data</i>
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 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.

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.

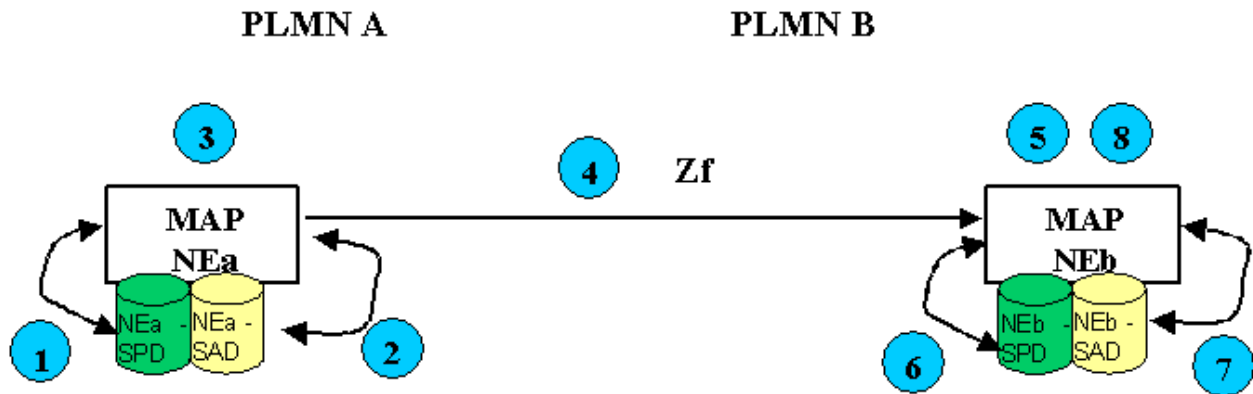


Figure 1. MAPsec Message Flow

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.
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 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.

Annex C (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
June 2001	SP_12	SP-010322			Presented to TSG SA #12 and approved (Release 4)	2.0.0	4.0.0
Sept 2001	SP_13	SP-010496	001		All messages of the same application context shall be applied MAPsec or not at all	4.0.0	4.1.0
Sept 2001	SP_13	SP-010497	002		Clarification of Scope	4.0.0	4.1.0
Sept 2001	SP_13	SP-010498	005	1	Clarifications in SPD and SAD contents	4.0.0	4.1.0
Sept 2001	SP_13	SP-010499	007		MAPsec Message Flow including extra SPD table	4.0.0	4.1.0
Sept 2001	SP_13	SP-010500	008	1	Correction to security policy requirements	4.0.0	4.1.0
Sept 2001	SP_13	SP-010501	009		Content and identifiers of a MAPSec SA	4.0.0	4.1.0
Sept 2001	SP_13	SP-010502	010		MIA key length unspecified	4.0.0	4.1.0
Sept 2001	SP_13	SP-010503	011		MAC calculation in PM2	4.0.0	4.1.0

History

Document history		
V4.0.0	June 2001	Publication
V4.1.0	September 2001	Publication