3GPP TS 33.200 V0.6.0 (2001-05)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group SA3
3G Security;
Network Domain Security;
MAP application layer security
(Release 4)

Keywords
Security, Core Network, MAP, Key management

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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 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 to/from, inside and between core networks. The security services that have been identified as being needed 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].

This specification applies to MAP version 3, TS 29.002 [4] Rel-4 and higher.

NOTE: It is explicitly noted that the automated key management and key distribution parts of MAPsec 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.

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

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

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

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

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, 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:

Zf MAPsec interface between networks/security domains for secure MAP-NE interoperation.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
IP	Internet Protocol
IV	Initialisation Vector
MAC	Message Authentication Code
MAP	Mobile Application Part
MAP-NE	MAP Network Element
MAPsec	MAP security – the MAP security protocol suite
NDS	Network Domain Security
NE	Network Entity
SA	Security Association
SADB	Security Association Database (sometimes also referred to as SADB)
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
TVP	Time Variant Parameter

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.

Before protection can be applied, Security Associations (SA) need 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.

A central concept introduced in this technical specification is the notion of a security domain. Within a security domain the same level of security and usage of security services is applied. For MAP application layer security, only one security domain shall exist per PLMN.

Editors Note: This needs to be reformulated to indicate that security policies are set up between pairs.

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-security domain.

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.

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.

Editors Note: Need to add flows from old Annex A.

5.3 MAPsec security association attribute definition

The following MAP security association attributes are defined:

- **Encryption Algorithm Identifier:**

  Identifies the encryption algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. Mapping of algorithm identifiers is defined in section 5.6.

Editor's Note: Format to be defined..

It is 4 bits.

- **Encryption Key:**

  Contains the encryption key. Length is 128 bits.

Editor's Note: Format to be defined.

- **Integrity Algorithm Identifier:**

  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.

Editor's Note: Format to be defined.

It is 4 bits.

- **Integrity Key:**

Contains the integrity key. Length is 128 bits.

Editor's Note: Format to be defined.

- **Protection Profile Identifier:**

  Identifies the protection profile. Length is 16 bits. Mapping of profile identifiers is defined in section 6.

Editor's Note: Format to be defined.

- **Fallback to Unprotected Mode Indicator:**

  In the case that protection is available, this parameter indicates whether fallback to unprotected mode is allowed.

Editor's Note: Format to be defined.

- **SA Lifetime:**

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

Editor's Note: Format to be defined.

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

5.3.1 Policy requirements for the MAPsec SPD

The security policies for MAPsec key management are specified in the NE's SPD. SPD entries define 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.

Editors Note: Need to add a table to define the SPD entries, include/clarify Fallback allowed indicator. Policy for SA renewal needed SA_Start, etc. Need to include separate SPDs for inbound and Outbound.

5.4 MAPsec structure of protected messages

5.4.1 MAPsec protection modes

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 operation protected by means of MAPsec consists 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 (see chapter 5.4.4). For integrity and authenticity in protection modes 1 and 2, 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. In protection mode 0 no protection is offered, therefore the protected payload is identical to the payload of the original MAP message.

5.4.2 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.

~~For cases where Protection Mode 0 is to be used the protection level will be identical to the original unprotected MAP message.~~ It is ~~therefore~~ allowed as an implementation option to let Protection Mode 0 operations be sent without the security header. (ed. note: Is this possible?)

5.4.3 Protection Mode 1

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

Cleartext|| f7~~H~~(Security Header||Cleartext)

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

- Cleartext
- Message authentication code calculated by the function f7~~Integrity Check Value~~

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function f7~~H~~ with the integrity key defined by the security association to the concatenation of Security Header and Cleartext. Length of the MAC is 4 octets.

~~Editor's Note: Length of the MAC needs to be defined.~~

5.4.4 Protection Mode 2

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

F6~~E~~(Cleartext) || f7~~H~~(Security Header|| f6~~E~~(Cleartext))

where "Cleartext" is the original MAP message payload in clear text. Confidentiality is achieved by encrypting Cleartext 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) function f7~~H~~ with the integrity key defined by the security association to the concatenation of Security Header and Ciphertext~~encrypted Cleartext~~. Length of the MAC is 4 octets. The length of the Ciphertext is the same as the length of the Cleartext.

~~Editor's Note: Length of the MAC needs to be defined.~~

5.5 MAPsec security header

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

- **TVP:**

4 octets time-stamp used for replay protection. The TVP 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:**

7~~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.)

Editor's Note: The scheme for allocating or calculating the NE-Id is to be defined.

- **Proprietary field (Prop):**

4 octet used to create different IV values for different protected MAP messages within the same TVP period. 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 formed from the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the destination network.

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

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

- **Original Component identifier:**

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

Ed. note: It may give information out of encrypted message

5.6 MAPsec algorithms

5.6.1 Mapping of MAP-SA algorithm identifiers

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

Table 3: MAPsec integrity algorithm identifiers

Integrity algorithm identifier	Description
0000	Null
0001	AES in a CBC MAC mode (MANDATORY)
-not yet assigned-	-not yet assigned-

~~Editor's Note: Should a null algorithm be defined.~~

Editor's Note: More specification on the mode of operation is required.

The algorithm 0001 is ISO 9797 Part I: padding method 2, MAC algorithm 1 (initial transformation =1, output transformation =1). No IV used.

Table 4: MAPsec encryption algorithm identifiers

Encryption algorithm identifier	Description
0000	Null
0001	AES in a stream cipher mode (MANDATORY)
-not yet assigned-	-not yet assigned-

~~Editor's Note: Should a null algorithm be defined.~~

Editor's Note: More specification on the mode of operation is required.

The algorithm 0001 is ISO 10116 Counter Mode with the parameter j = 128 bits, SV =IV and truncation of the last block is according to the method in the Annex A 5.3.

5.6.2 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 padding shall be 1 octet of zero bits. Ed. note: this is the best choice for Counter mode.

~~Editor's Note: Padding rules to be defined.~~

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 5: 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

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

6.2.3 MAP-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

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

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

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

NOTE: This protection group is incomplete.

6.2 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.

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

Table 11: Protection profile encoding

The following protection profiles are defined.

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		✓	✓	✓	✓

Table 12: Protection profile definition

Editor's note: Profiles B and C are different to those specified in the Siemens contribution S3-010192.

Annex A (informative): Guidelines for manual key management

A.1 Inter-domain Security Association and Key Management Procedures (Zd-interface)

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 defined how to carry out the initial exchange of MAPsec SAs
- to defined 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)

A.2 Local Security Association Distribution (Ze-interface)

Manual Local Security Association Distribution is executed entirely within one security domain[1] and is consequently at the discretion of the security domain administrative authority.

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

- MAPsec may be **required** or it may be **optional** towards other MAP-NEs. Procedures to set this information in the MAP-NEs on a per security domain destination basis must be provided. This information should available to the MAP-NE before any communication towards other MAP-NEs is to take place. MAP-NEs capable of executing MAPsec should define a default value for the MAPsec **required/optional** parameter.
- 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 (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New

[1] Operators are expected define one security domain per network
