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

An identified security weakness in 2G systems is the absence of security in SS7 networks. 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.

~~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 key management and distribution procedures. The key management interfaces and mechanisms are not part of Rel4, but an outline of the MAPsec key management and distribution architecture is included in annex A for information.~~

~~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, and MAPsec will therefore also apply should MAP be ported to IP based networks.~~

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, and MAPsec will therefore also apply should MAP be ported to IP based networks.

~~The scope of the UMTS network domain control plane is to cover the control signalling in the UMTS core network. This includes both the SS7 and IP based control plane signalling protocols. The present document defines the MAP security architecture for the UMTS network domain control plane.~~

~~The UMTS core network contains a number of SS7 based protocols, which in this specification are referred to as legacy protocols. While the stated goal of the network domain security is to cover all of the core network protocols, only MAP will be protected in Rel4. Behind this is a realization that SS7 based legacy protocols can in practice only be protected at the application layer, and that the work involved in protecting the legacy protocols therefore will be high and require redesign of the protocol itself. Even in the cases were it would be technically feasible to do the job it is questionable whether the benefits would ever justify the required effort. Consequently, the only legacy protocol that is protected in Rel4 is the MAP protocol [4].~~

NOTE-1: It is explicitly noted that the automated key management and key distribution parts of MAPsec is not part of Rel4. All key management and key distribution in Rel4 must therefore be carried out by other means. (See Annex B)

~~NOTE-1: MAP inter-operator key management and local key distribution are part of Rel5.~~

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of 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] 3G TS 29.060: GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface

[6] 3G TS 33.102: Security Architecture

[7] 3G TS 33.103: Security Integration Guidelines

[8] 3G TS 33.120: Security Objectives and Principles

[9] RFC-2401: Security Architecture for the Internet Protocol

[10] RFC-2406: IP Encapsulating Security Payload

[11] RFC-2407: The Internet IP Security Domain of Interpretation for ISAKMP

[12] RFC-2408: Internet Security Association and Key Management Protocol (ISAKMP)

[13] RFC-2409: The Internet Key Exchange (IKE)

[14] RFC-2412: The OAKLEY Key Determination Protocol

[15] draft-arkko-map-doi-01.txt: The MAP Security Domain of Interpretation for ISAKMP

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~~n SA~~ 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:

C	MAP interface between an HLR and an MSC
D	MAP interface between an HLR and a VLR
E	MAP interface between MSCs
Gc	Interface between a GGSN and an HLR
Gr	Interface between an SGSN and an HLR
Zd	MAPsec interface between KACs belonging to different networks/security domains
Ze	MAPsec interface between KACs and MAP-NEs within the same network
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
DES	Data Encryption Standard
DoI	Domain of Interpretation
ESP	Encapsulating Security Payload
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security - a collection of protocols and algorithms for IP security incl. key mngt.
ISAKMP	Internet Security Association Key Management Protocols
IV	Initialisation Vector
KAC	Key Administration Centre
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
SAD	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 Overview over UMTS network domain security for SS7 based protocols

4.1 Introduction

The scope of this section is to outline the basic principles for the ~~network domain~~MAP application layer security architecture. ~~A central concept introduced in this specification is the notion of a network security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks and hence separate security domains.~~

4.2 Protection at the application layer

If SS7 based protocols are to be protected then they shall be protected at the application level. As a general~~the main~~ rule, protocols that can be transported by either SS7 or IP networks shall be protected at the application layer. SS7 or mixed SS7/IP based protocols will commonly be referred to as legacy protocols in this specification.

It is recognised that legacy protocols may also be protected at the network layer when using IP as the transport protocol. However, whenever inter-working with networks using SS7-based transport is necessary, protection at the application layer shall be used.

Security Associations (SA) define, among other things, which keys, algorithms, and protection profiles to use to protect MAP signalling. For legacy protocols, the necessary ~~security associations~~ MAP-SAs between networks are negotiated between ~~Key Administration Centre entities~~the respective network operators. The negotiated SA will be effective network-wide and distributed to all affected network elements. 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. ~~The network operator may have more than one KAC in its network in order to avoid a single point of failure or for performance reasons. A KAC may be defined for interaction towards all reachable security domain destinations or it may be defined for only a subset of the reachable destinations.~~

NOTE-1: It is explicitly noted that the automated key management and key distribution parts of MAPsec ~~is~~ are not part of Rel4. All key management and key distribution in Rel4 must therefore be carried out by other means. (See Annex B)

~~4.3 Security for SS7 and mixed SS7/IP based protocols~~

~~As the general rule, legacy protocols shall be protected at the application layer.~~ Protection at the application layer ~~This~~ implies changes to the application protocol~~s themselves~~ itself to allow for the necessary security functionality to be added.

This 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 has been recognised that legacy protocols may also be protected at the network layer when using IP as the transport protocol. However, whenever interworking with networks using SS7-based transport is necessary then protection at the application layer shall be used.~~

4.43 Security domains

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 network (i.e. per PLMN).

4.4.1 Security domains andl interfaces

The UMTS network domain shall be logically and physically divided into security domains. These control plane security domains may closely correspond to the core network of a single operator.

The specific network domainMAP application layer security interfaces for MAP isare found in table 1. Annex -A contains a more detailed description of Key Administration Centres (KACs), and the Zd and Ze- interfaces.

Note: The KAC and the Zd and Ze interfaces are not standardised in Rel4.

Table 1: Network domainMAP application layer security specific interfaces

Interface	Description	Network type
Zd	Network domain security interface between networks. The Zd-interface is defined for negotiation of MAP security associations between KACs.	IP
Ze	Network domain security interface between KAC and MAP-NE within the same network. The interface is security protected by means of an IPsec ESP tunnel.	IP
Zf	Network domain security interface between MAP-NEs engaged in security protected signalling (applies to MAP-NEs belonging to different or even to the same security domain)	SS7/MAP

The interfaces, which affects/isare affected by this technical specification are described in the table below. Notice that when security protection is employed over an interface, this specification will refer to the Z-interface name.

NOTE: It is explicitly noted that only the Zf-interface is defined for Rel4. The Zd and Ze interfaces only apply to Rel5, but is included here for information.

Table 2: Interfaces that are affected by network domain MAP application layer security

Interface	Description	Affected protocol	Security implication
C	Interface between HLR and MSC	MAP	MAPsec shall be supported
D	Interface between HLR and VLR	MAP	MAPsec shall be supported
E	Interface between MSC and MSC	MAP	MAPsec shall be supported
G	Interface between VLR and VLR	MAP	MAPsec shall be supported
Gc	Optional interface between GGSN and HLR	MAP	MAPsec shall be supported
Gr	Interface between SGSN and HLR	MAP	MAPsec shall be supported

5 MAP security (MAPsec)

5.1 Security services afforded provided by MAPsec

The security services required for SS7 and mixed SS7/IP-based protocols 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 be able to perform the following operations:

~~Request MAP-SA information to the KAC. This is done according to the "RequestSA" procedure outlined in Annex A.2~~

~~Supervise MAP-SA lifetimes to initiate new valid SA information once the SA in use has expired. Optionally, the MAP-NE might request new SAs before the previous SAs have expired~~

- Secure MAP signalling (i.e. send/receive protected or unprotected messages) according to ~~MAP-SA~~ information in NE-SPD-MAP and NE-SADB-MAP~~received from the KAC~~

MAPsec MAP-NEs shall be responsible for the maintenance of the following databases:

- NE-SPD-MAP: A database in an NE containing MAP security policy information.
- NE-SADB-MAP: A database in an NE containing MAP-SA information. MAP-NEs shall control the SAs lifetime and expired SAs shall be deleted from the database

~~NE-SADB-MAP: A database in a NE containing MAP-SA information received from the KAC in the course of a "RequestSA" procedure. MAP-NEs shall control the SAs lifetime and the expired SAs shall be deleted of the database~~

~~(Optional) NE-SADB-IP: Containing IPSec-SAs for protection of IP traffic between the KAC and NEs over the Ze interface~~

~~5.3 MAPsec Domain of Interpretation~~

~~Key management and distribution between operators for MAPsec is done by means of the Internet Key Exchange (IKE). To adapt IKE for use with MAPsec a MAPsec Domain of Interpretation (DoI) document is required. Such document is to defined and published within the IETF framework as a separate RFC. Currently the MAPsec DoI has the status of a draft RFC ([15]). Since the MAPsec DoI RFC is only concerned with non-IP issues it will be an informational RFC, but it shall nevertheless be normative for 3GPP MAPsec purposes.~~

~~5.3.1 MAPsec DoI requirements~~

~~ISAKMP (RFC-2408, [12]) places the following significant requirements on a DoI definition:~~

- ~~Define the interpretation for the Situation field~~
- ~~Define the set of applicable security policies~~
- ~~Define the syntax for DoI-specific SA Attributes (Phase II)~~
- ~~Define the syntax for DoI-specific payload contents~~
- ~~Define additional Key Exchange types, if necessary~~
- ~~Define additional Notification Message types, if needed~~

~~The normative MAPsec DoI definitions are found in the MAPsec DoI RFC ([15]). In addition to this Annex C contains complementary MAPsec definitions.~~

5.3~~3.2~~ MAPsec Security Association Attributes

To allow automated SA establishment to be introduced using the IETF IKE protocol, MAPsec Security Associations are defined according to a MAP Domain of Interpretation for IKE which is currently available as an Internet Draft [15]. The MAPsec DoI is required to be issued as an IETF RFC. Since the MAPsec DoI is only concerned with non-IP issues it will be an informational RFC, but it shall nevertheless be normative for 3GPP MAPsec purposes.

The following MAP security association attributes are defined in the MAPsec DOI:

~~The following attributes are needed~~

- ~~Protection Profile~~
- ~~Authentication algorithm for integrity and authentication~~
- ~~Encryption algorithm for confidentiality~~
- ~~Encryption and authentication keys~~
- ~~SA lifetime~~

- **Encryption Algorithm Identifier:**

  Identifies the encryption algorithm. Section 5.6 defines the algorithms that are assigned to the MAPsec DoI TransformID

- **Encryption Key:**

  Contains the encryption key. 128 bits. Format defined in MAPsec DOI

- **Integrity Algorithm Identifier:**

  Identifies the integrity algorithm. Section 5.6 defines the algorithms that are assigned to the MAPsec DoI TransformID

- **Integrity Key:**

  Contains the integrity key. 128 bits Format defined in MAPsec DOI

- **Protection Profile Identifier:**

  Identified the protection profile. 16 bits (format defined in section 6?)

- **Fallback to Unprotected Mode Indicator:**

  In case protection is required, this parameter indicates whether fallback to unprotected mode is allowed. Format defined in MAPsec DOI.

- **SA Lifetime:**

  Defines the actual duration of the SA. The expiry of the lifetime shall be given in absolute time. Format defined in MAPsec DOI.

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.~~3.3~~4 Policy requirements for the MAPsec SPD

~~The policy is described as in the RFC-2401 [9] with following changes:~~

- ~~The lifetime of the MAP SA is not defined as an amount of data transferred, but as absolute lifetime in seconds.~~
- ~~The generated MAP SA will not be used for processing inbound and outbound traffic in KACs and thus processing choices *discard*, *bypass IPsec* and *apply IPsec* does not apply.~~

- ~~The operator defines for which networks MAPsec SA's are negotiated.~~

The security policies for MAPsec key management are specified in the ~~KACs'~~ NE's SPD ~~by the network operator~~. SPD entries define which MAP SAs (if any) to use to protect MAP signalling based on the PLMN of the peer NE. ~~The SPDs in the network elements are derived from the SPD of the KAC in the network.~~ There can be no local security policy definitions for individual NEs. Instead, SPD entries of different NE within the same PLMN shall be identical.

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.

5.4.3 Protection Mode 1

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

TVP||Cleartext|| H(TVP|| Security Header||Cleartext)

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

- Time Variant Parameter TVP
- Cleartext
- Integrity Check Value

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity key defined by the security association to the concatenation of Time Variant Parameter TVP, Security Header and Cleartext.

The TVP used for replay protection of Secured MAP operations is a 32-bit time-stamp. The receiving network entity shall 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 must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

NOTE: A more detailed specification is required on the IV structure.

NOTE: Lengths of parameters need to be defined here as agreed in Madrid (key 128bit, MAC 64 (or 32-63 if needed)).

5.4.4 Protection Mode 2

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

TVP|| E(Cleartext) || H(TVP|| ||Security Header|| 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. Authentication of origin and integrity are achieved by applying the message authentication code (MAC) function H with the integrity key defined by the security association to the concatenation of Time Variant Parameter TVP, Security Header and encrypted Cleartext.

The TVP used for replay protection of Secured MAP messages is a 32-bit time-stamp. The receiving network entity shall accept a message only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

NOTE: A more detailed specification is required on the IV structure.

NOTE: Lengths of parameters need to be defined here as agreed in Madrid (key 128bit, block length 128 bit, MAC 64 (or 32-63 if needed)).

It is recommended to use protection mode 2 whenever possible as this makes replay attacks even more difficult.

5.5 MAPsec security header

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

- **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.

- **Initialisation Vector (IV):**

  Initialisation vectors are used with block ciphers in chained mode to force an identical plaintext to encrypt to different cipher texts. Using IVs prevents launching a codebook attack against encrypted traffic. The IV has only local significance in the MAP-NE.

  NOTE: Whether the Initialisation Vector is needed depends on the mode of operation of the encryption algorithm.

  NOTE: A more detailed specification is required on the IV structure.

- **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).

5.6 MAPsec algorithms

NOTE: Algorithm interface may need to be defined.

An algorithm indication field is used to identify the actual algorithms to be used. The MAPsec Integrity Algorithm (MIA) will be assigned to the MAPsec DoI TransformID.

Table 3: MAPsec Integrity Algorithm identifiers

MIA identifier	Description
00	Null
01	AES in CBC MAC mode (MANDATORY)
-not yet assigned-	-not yet assigned-

NOTE: If the FIPS AES-MAC mode is not available in time then the ISO CBC-MAC mode could be used.

The MAPsec Encryption Algorithm (MEA) will be assigned to the MAPsec DoI TransformID

Table 4: MAPsec Encryption Algorithm identifiers

MEA identifier	Description
00	Null
01	AES (MANDATORY)
-not yet assigned-	-not yet assigned-

NOTE: More specification on the mode of operation of AES is required. The working assumption is FIPS CBC mode (or AES in ISO CBC mode if different?).

For both MIA and MEA the minimum key length shall be 128 bits.

~~Annex C (normative):~~
~~Additional definitions for MAPsec DoI~~

~~The definitions contained in this annex are to be complementary to the definitions found in the MAPsec DoI RFC ([15]).~~

~~C.1 MAPsec SA definition~~

~~[EDITOR: We need to precisely define the MAPsec SA.]~~

~~C.2 Additional definitions for MAPsec DoI~~

~~[EDITOR: The S3#17bis NDS ad-hoc decided to split the MAPsec DoI into two parts. The main reason for this was to avoid having to update the MAPsec DoI RFC when the changes only really affected 3GPP MAPsec. So this annex is then to contain definitions that only applies to MAPsec and which S3 may change without having to update the RFC.~~

~~Needless to say: **CONTRIBUTIONS WANTED**]~~