3GPP TS 33.200 V0.4.0 (2001-04)

Technical Specification

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

Keywords
Security, Core Network, 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 the SS7 networks has been ~~An identified~~ identified as potential security ~~weakness~~ risk in 2G systems ~~is the absence of security in SS7 networks~~. Since originally the SS7 networks were the provinces of a small number of large institutions, t~~T~~his was ~~formerly~~ perceived not to be a serious security problem~~., since the SS7 networks were the provinces of a small number of large institutions~~. This is no longer the case, ~~and~~therefore the ~~so there is now a~~ need for security ~~precautions~~considerations has been identified as a high priority item for 3GPP networks. Another significant development has been the introduction of IP as the network layer in the GPRS backbone network and then later in the UMTS network domain, i.e., ~~. Furthermore,~~ IP protocol is ~~not only~~ used for signalling traffic as well as ~~, but also~~ for user traffic. Therefore, t~~T~~he introduction of IP ~~therefore~~ signifies not only a shift towards packet switching, which is a major change by its own accounts, but also a shift towards completely open and easily accessible protocols. The implication is that, from a security point of view, a whole new set of threats and risks must be ~~faced~~addressed.

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

Various protocols and interfaces are used ~~for~~to ~~control~~control the signalling plane ~~signalling, to/from~~, ~~inside and between~~inter as well as intra core network~~s~~. The following ~~security services that~~ have been identified as essential: ~~as being needed are~~ confidentiality, integrity, authentication and anti-replay protection. ~~These will be ensured~~The security services will be ~~by standard procedures~~standardized, based on industry acceptable cryptographic techniques.

1 Scope

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

The UMTS core network contains a number of SS7 based protocols, which ~~in this specification~~ are referred to as "legacy protocols" in this specification document. While the stated goal of the network domain security is to cover all ~~of the~~ core network protocols, not all ~~of the~~ legacy protocols will be protected in Rel4 timeframe. This decission has been made ~~Behind this is a realization that~~due to practical technical and commercial constraints, i.e., the SS7 ~~based~~ legacy protocols can ~~in practice only~~realistically be protected only at the application layer. Protecting the SS7 network at a lower layer will require large development efforts, including the redesign of the ~~, and that the work involved in protecting the legacy protocols therefore will be high and require redesign of the~~ current SS7 protocol itself. Even ~~in the cases were it would~~if this development is ~~be~~ technically feasible, ~~to do the job~~ it is questionable whether the commercial benefits ~~would~~ can ever justify the required development effort. ~~Consequently~~Therefore, the ~~only~~ only "legacy protocol" that shall be~~is~~ protected in Rel4 is the MAP protocol [4].

NOTE-1: Lawful Interception considerations and requirements are covered in separate specifications [8,9].

NOTE-2: 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 33.106: Lawful interception requirements

[9] 3G TS 33.107: Lawful interception architecture and functions

[10] 3G TS 33.120: Security Objectives and Principles

[11] 3G TR 33.800: Principles for Network Domain Security

[12] RFC-2393: IP Payload Compression Protocol (IPComp)

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

[14] RFC-2402: IP Authentication Header

[15] RFC-2403: The Use of HMAC-MD5-96 within ESP and AH

[16] RFC-2404: The Use of HMAC-SHA-1-96 within ESP and AH

[17] RFC-2405: The ESP DES-CBC Cipher Algorithm With Explicit IV

[18] RFC-2406: IP Encapsulating Security Payload

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

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

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

[22] RFC-2410: The NULL Encryption Algorithm and Its Use With IPsec

[23] RFC-2411: IP Security Document Roadmap

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

[25] RFC-2451: The ESP CBC-Mode Cipher Algorithms

[26] RFC-2521: ICMP Security Failures Messages

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

[28] ITU-T **Recommendation Q.700 (03/93) - Introduction to CCITT signalling system No. 7**

[29] ITU-T **Recommendation Q.701 (03/93) - Functional description of the message transfer part (MTP) of signalling system No. 7**

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~~ goal is to protect against an authorized ~~replay~~ retransmission of ~~self-contained packets~~a captured data unit ~~that already have a cryptographical integrity mechanism in place.~~ The data unit may have been validated via a cryptographical integrity mechanism.

Data C~~c~~onfidentiality: The property that the ~~information~~ data flow is ~~not made available or disclosed to~~protected from disclosure to an unauthorised individuals, entities or processes. Data confidentiality is supported by encryptions algorithms that convert a plain text message into an encrypted message (or ciphertext).

Data integrity: The property that ensures that messages are received as sent, with no duplication, insertion, modification, reordering or replay.~~data has not been altered in an unauthorised manner~~. Data integrity is provided by calculating a cryptographic (e.g., Keyed Hashing) message digest (called Message Authentication Code or MAC) based on the message content. Any changes in the message content will trigger a corresponding change in the message MAC.

Data origin authentication: The corroboration that the message is from the source ~~of data received is as claimed~~that is claims to be from.

Entity authentication: The provision of assurance of the claimed identity of an entity.

IPSec SA: provide security services at the IP layer and is enabling a system to select required security protocols: Authentication Header (AH) or Encapsulation Security Protocol (ESP), determine the algorithms to be used, the transforms, the keys, and the duration for which the keys are valid. The IPSec is stored in a SA Database (SADB), it is protocol specific and unidirectional. If a pear relationship is needed, then two security associations are required:

- **Security Parameter Index (SPI)** A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- **IP Destination Address** : the address of the destination endpoint of the SA (e.g., end user, or network entity).
- **Security Protocol Identifier**: indicates whether the association is an AH or ESP security association.

Key freshness: A key is fresh if it can be guaranteed to be new (i.e., the key shall not be reused~~, as opposed to an old key being reused~~ through actions of either an adversary or authorised party).

Legacy protocols: Network utilizing SS7 or mixed SS7/IP based protocols will be commonly referred to as" within this document

MAP: TCAP carries **Mobile Application Part** (MAP) messages sent between mobile switches and databases to support user authentication, equipment identification, and roaming.

Security Association (SA): A one-way relationship between the sender and the receiver that ensures the security of the traffic carried on.~~uni-directional logical connection created for security purposes~~. All traffic traversing a~~n~~ SA is ~~provided~~protected by the same security protocol ~~protection~~. **~~(this does not apply to IKE security association)~~**

SS7: Common Channel Signalling System #7 (SS7) is a global telecommunications standard (defined by ITU-T) for the signalling system that allows the various components of a telephone network to exchange information and connect calls. Used in both wireless and wireline networks

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
F	MAP interface between a MSC and an EIR
Gc	Interface between a GGSN and an HLR
Gd	Interface between an MSC and an SGSN
Gf	Interface between an SGSN and an EIR
Gi	Reference point between GPRS and an external packet data network
Gn	Interface between two GSNs within the same PLMN
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs
Gr	Interface between an SGSN and an HLR
Gs	Interface between an SGSN and an MSC/VLR.
Iu	Interface between the RNS and the core network. It is also considered as a reference point.
Iur	Interface between RNSs in the access network
Za	Interface between SEGs belonging to different networks/security domains
Zb	Interface between SEGs and NEs within the same network/security domain
Zc	Interface between NEs within the same network/security domain
Zd	Interface between KACs belonging to different networks/security domains
Ze	Interface between KACs and MAP-NEs within the same network
Zf	Interface between networks/security domains for secure interoperation. MAP-NE ←→MAP-NE.

3.3 Abbreviations

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

AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
BG	Border Gateway
CS	Circuit Switched
DES	Data Encryption Standard
DoI	Domain of Interpretation
ESP	Encapsulating Security Payload

GTP	GPRS Tunnelling Protocols
IESG	Internet Engineering Steering Group
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
NAT	Network Address Translator
NDS	Network Domain Security
NE	Network Entity
PS	Packet Switched
RNS	Radio Network Subsystem
SA	Security Association
SAD/SADB	Security Association Database (sometimes also referred to as SADB)
SEG	Security Gateway
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
SS7	`Signalling System no. 7 protocol
TVP	Time Variant Parameter
USP	UMTS Security Profile

4 Overview over UMTS network domain security

4.1 Introduction

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

In this specification, a distinction is made between protocols using SS7 based networks and IP based networks as their transport mechanism ~~are made~~. Ideally no such distinction should have had to be made, but ~~the~~ technical differences between the SS7 and IP architectures ha~~ves~~ forced the following high-level sub-sectioning:

- **If native IP based ~~protocols~~ networks are to be protected, they shall be protected at the network level by means of the IPsec protocols**

  The UMTS network domain control plane is ~~also sectioned~~subdivided into multiplesecurity domains. ~~and t~~Typically th~~ose domain ese coincide~~align with an operator's service area borders. The border between the security domains is protected by Security Gateways (SEGs). The SEG~~s are~~ is responsible for enforcing the security policy of it's own~~a~~ security domain ~~towards~~ in relationship to all other SEG associated with ~~s in~~ the destination security domain. The network operator may have ~~more than one~~multiple SEGs in its network in order to avoid a single point of failure (i.e., redundancy) or for performance reasons (e.g., distributed processing). ~~A~~ One SEG may be ~~defined~~ associated with ~~for interaction towards~~ all reachable security domain destinations or it may be defined for only a subset of the reachable destinations.

  The UMTS network domain security does not extend to the user plane and consequently the security domains and the associated security gateways towards other domains do no encompass the user plane Gi interface ~~towards other, possibly external to UMTS, IP networks.~~.

- **If a networks using SS7 protocol ~~based protocols are~~ is to be protected, ~~they~~ it shall be protected at the Mobile Application Part (MAP)~~application~~ level**

  ~~As the main rule, p~~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 be commonly ~~be~~ referred to as "legacy protocols" ~~in~~ within this ~~specification~~document.

  For legacy protocols, the necessary security associations (SA) between networks are negotiated between Key Administration Centre (KAC) entities. The negotiated SA will be ~~effective~~ enforced network-wide and distributed to all ~~affected~~ relevant network elements. For routing purposes, the ~~S~~signalling traffic, which is ~~-~~protected at the application layer ~~will, for routing purposes,~~ will be indistinguishable from unprotected traffic to all intermediate nodes, ~~parties~~ except for the sending and receiving entities. In order to avoid a single point of failure or for performance reasons, ~~The~~ a network operator may have more than one KAC in ~~its~~ his/her network ~~in order to avoid a single point of failure or for performance reasons~~. A KAC may be ~~defined~~assigned ~~for~~ to control the security interaction ~~towards~~ among all the reachable security domain destinations or it may be defined for only a subset of the reachable domain destinations.

NOTE-1: It is explicitly noted that protection for IP based protocols is not part of Rel4. Protection for IP based protocols ~~will first be introduced in~~is targeted for Rel5 of this technical specification.

NOTE-2: 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.

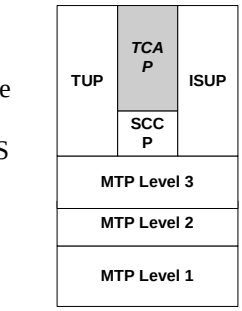
4.2 Security for SS7 and mixed SS7/IP based protocols

Legacy protocols shall be protected at the application layer (i.e., MAP layer). This ~~implies~~ requires changes to the application protocols themselves to ~~allow~~ provide ~~for~~ the necessary security functionality. This ~~specification~~ document contains the stage-2 specification required to provide ~~for the~~ security protection ~~of~~ to the legacy protocols. The actual implementation (stage-3) specification can be found in the specification associated with ~~for~~ the target protocol.

Overview over security protected SS7 based protocols for Rel4:

- **Mobile Application Part** (MAP)

  ~~S~~ecurity for MAP messages (carried within TCAP messages) shall be provided by the MAP security protocol. The MAP security protocol stage-2 specification ~~is~~ can be found in section 7 and Annex B.1 and the stage-3 specifications ~~is~~ can be found in TS 29.002 [4].



SS7 Protocol Stack

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

4.3 Security for native IP based protocols

NOTE: This is a placeholder for the Rel5 version of the specification.

4.4 Security domains

4.4.1 Security domains and interfaces

The UMTS network domain shall be logically and physically divided into security domains. ~~These~~ The control plane security domains, which may closely correspond to the core network of a single operator, ~~shall be separated~~may interface with other control plane domains via ~~by means of~~ security gateways (SEG).

The specific network domain security interfaces is found in table 1. Section 5.2 contains a detailed description of the Z-interfaces.

Table 1: Network domain security specific interfaces

Interface	Description	Network type
Za	Network domain security interface between SEGs. The interface is used for both the negotiation of security associations and for the set-up of ESP protected tunnels between SEGs (no third party negotiation).	IP
Zb	Network domain security interface between SEGs and NEs within the same network. The interface is used for both the negotiation of security associations and for the set-up of an ESP protected tunnel.	IP
Zc	Network domain security interface between NEs within the same network. The interface is used for both the negotiation of security associations and for the set-up of an ESP protected tunnel.	IP
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/is affected by the network domain security 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 remaining interfaces only applies to Rel5, but is included here for information.

Table 2: Interfaces that are affected by network domain 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
F	Interface between MSC and EIR	MAP	MAPsec shall be supported
G	Interface between VLR and VLR	MAP	MAPsec shall be supported
J	Interface between HLR and gsmSCF	MAP	MAPsec shall be supported
Gc	Optional interface between GGSN and HLR	MAP	MAPsec shall be supported
Gd	Interface between SMS-MSCs and SGSN	MAP	MAPsec shall be supported
Gf	Interface between SGSN and EIR	MAP	MAPsec shall be supported
Gn	Interface between GSNs within the same network	GTP	ESP shall be supported
Gp	Interface between GSNs in different PLMNs.	GTP	IPsec shall be supported. Security Gateways shall be present at the domain borders.
Gr	Interface between SGSN and HLR	MAP	MAPsec shall be supported

NOTE-1: The requirement for MAPsec support is dependent on the MAPsec security profile.

NOTE-2: The Iu and Gs interfaces are presently not covered by NDS.

NOTE-3: It is explicitly noted that only the MAP interfaces are covered by Rel4. Coverage for the GTP interfaces will be introduced with Rel5 of this specification.

4.5 Security Gateways (SEGs)

NOTE: This is a placeholder for the Rel5 version of the specification.

4.6 Key Administration Centres (KACs)

Key Administration Centres (KACs) are network entities ~~that are used for~~ negotiating MAPsec SAs on behalf of MAP-NEs. The KACs are defined to ~~handle~~ support secure communication over ~~these interfaces~~the:

- the Zd-interface ~~, which is located~~ between KACs ~~from~~ associated with different MAP security domains. ~~The~~ Internet Key Exchange (IKE) protocol with support for MAPsec DoI shall be used over this interface.
- the Ze-interface~~, which is located~~ between a KAC and a MAP-NE within the same MAP security domain is used to transfer MAPsec SAs from KACs to MAP-NEs. ~~The~~ IKE and the ESP protocols may be used to negotiate and secure the connection between the KAC and the MAP-NE.

When a MAP-NE ~~s~~ need~~s~~ to establish a secure connection ~~towards~~ with another MAP-NE ~~s they~~ it will request a MAPsec SA from the KAC. The KAC will then either provide an existing MAPsec SAs or negotiate a new MAPsec SA, before returning the MAPsec SA to the MAP-NE.

A MAPsec SA is valid for all MAP communication between the two security domains for which it ~~is~~ was negotiated. That is, the same MAPsec SA shall be provided to all MAP-NE in the same security domain (e.g., domain A) when communication with the MAP-NEs in a different security domain (e.g., domain B). Each security domain ~~can~~ may have one or more KACs. Each KAC will ~~be defined~~control ~~to~~ the MAPsec SAs ~~towards~~ associated with a ~~well-~~pre-defined set of reachable MAP security domains. The number of different KACs in a specific security domain ~~will~~ depend~~s~~ on the need to differentiate between the externally reachable destinations, the need to balance the traffic load and the need to ~~to~~ avoid a single point of failures.

The following are the most important tasks for a KAC:

- Perform MAP-SA negotiation with KACs belonging to other security domains. This action is triggered either by a NE's request for a MAP-SA ~~by a NE~~ or by a security policy enforcement directive. ~~when MAP-SAs always should be available.~~
- Perform refresh of a MAP-SA~~s~~. The refresh can be ~~T~~triggered internally by the MAP-SA lifetime supervision, ~~which is d~~based~~depending~~ on the policies set by ~~the~~ an operator ~~and if, it is~~ and ~~decided~~ established during the negotiation protocol.
- Distribute valid MAP-SAs to requesting nodes that belong~~ing~~ to the same network as the KAC. This is done according to the MAP-SA transport procedures defined in section 7.2.4.
- Establish ESP protected communication between itself and all other NEs in its own network

More information on KACs can be found in 5.3 and section 7.

KACs are responsible for managing and controlling security sensitive operations and shall be physically secured. They shall also offer capabilities for the secure storage of long-term keys used for IKE authentication.

NOTE: It is explicitly noted that Key Administration Centres are not part of Rel4 of MAPsec. Consequently, there is not requirement for a KAC in a Rel4 network.. KACs will be introduced in Rel5 of this specification and this section is only for information.

5 Key management and distribution architecture for the UMTS core network

5.1 Security Associations (SAs)

NOTE: This is a placeholder for the Rel5 version of the specification.

5.2 Use of the Internet Key Exchange protocol

NOTE: This is a placeholder for the Rel5 version of the specification.

5.3 UMTS key management and distribution architecture for native IP based protocols

NOTE: This is a placeholder for the Rel5 version of the specification.

5.4 UMTS key management and distribution architecture for SS7 and mixed SS7/IP-based protocols

The following section specifies the generic parts of the key management and distribution architecture for SS7 and mixed SS7/IP-based protocols. ~~Due to the fact that~~Since the security mechanisms is implemented at the ~~are found on the~~ application layer, a number of the issues are unique to ~~the applicat~~this implementation~~ion~~. Section 7 contains detailed and specific requirements for the applicable application protocols.

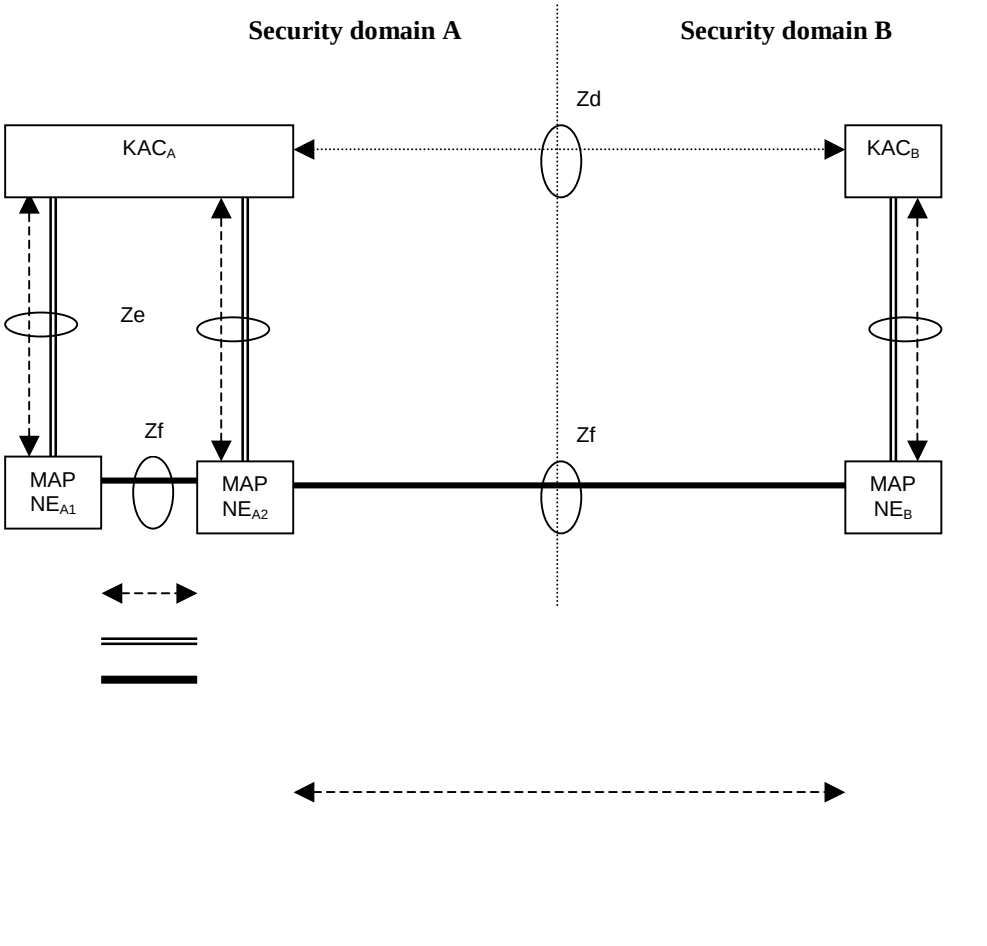


Figure 2: Overview of the Zd, Ze and Zf interfaces

~~For Rel4 the o~~Only SS7 MAP protocol ~~to be~~shall be protected in Rel4. ~~is the MAP protocol~~. References to MAP security (MAPsec) may ~~therefore~~ be ~~extended~~ expended to be more generic in later releases.

The following interfaces are defined MAPsec.

- **Zd-interface (KAC-KAC)**

  The Z-d-interface is used to negotiate MAPsec Security Associations (SAs) between MAP security domains. The traffic over Zd consists only of IKE negotiations. The negotiated MAPsec SAs are valid only ~~on~~ between two specific a security domain ~~to security domain basis~~.

- **Ze-interface (KAC-NE)**

The Ze-interface is ~~located~~ between MAP-NEs and a KAC ~~from~~ within the same MAP security domain. The KAC and the MAP-NE are ~~able~~ capable of ~~to~~ establishing and maintaining an ESP tunnel between them. Whether the tunnel is established when needed or a priori is for the MAP security domain operator to decide. The tunnel is subsequently used for transporting ~~of~~ MAPsec SAs from the KAC to the target MAP-NE.

- **The Zf-interface (NE-NE)**

The Zf-interface is ~~located~~ between MAP-NEs. The MAP-NEs may ~~be from the~~belong to the same security domain or ~~from~~ to different security domains (as shown in figure 2). The MAP-NEs use MAPsec SAs received from a KAC to protect the MAP operations. The MAP operations within the MAP dialogue are selectively protected, ~~selectively~~ as specified in the applied MAPsec security profile.

NOTE: It is explicitly noted that there is no Rel4 requirements for support of KACs or the associated Zd/Ze-interfaces. KACs and its associated interfaces and protocols will only be introduced in Rel5. For Rel4 this section is only for information.

6 Security for native IP based protocols

NOTE: This is a placeholder for the Rel5 version of the specification.

7 Security for SS7 and mixed SS7/IP based protocols

7.1 Security services afforded to the protocols

The security services required for SS7 and mixed SS7/IP-based protocols are:

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

7.2 MAP security (MAPsec)

This section describes mechanisms for establishing secure signalling links between MAP network entities

7.2.1 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~~shall be defined and published within the IETF framework as a separate RFC ([27]. Since the MAPsec DoI RFC ~~is~~ addresses only ~~concerned with~~ non-IP issues, it will be an informational RFC, but it shall nevertheless be normative for UMTS MAPsec purposes.

7.2.1.1 MAPsec DoI requirements

ISAKMP (RFC-2408, [20]) 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

IANA will not normally assign a DoI value without referencing some public specification, such as an Internet RFC. Without a DoI value assigned by IANA, the MAP SA negotiation over the interface Z_D is not possible. MAPsec DoI for ISAKMP draft *must* be written, since the new DoI is an essential part of the key management architecture.

The following sections define briefly the requirements for MAPsec DoI for ISAKMP.

7.2.1.2 MAPsec Situation definition

Within ISAKMP, the Situation provides information that the responder can use to determine how to process incoming SA request. For the MAPcec DoI, the Situation field is always left empty.

7.2.1.3 MAPsec Security Policy Requirements

The MAPsec DoI does not impose specific security policy requirements on any implementation.

MAPSec Assigned Numbers

The following sections list the Assigned Numbers for the MAPsec DoI: protocol identifiers and transform identifiers.

- **MAPsec Protocol Identifier** defines a value for the Security Protocol Identifier referenced in an ISAKMP Proposal Payload for the MAPsec DoI.

Protocol ID	Value
PROTO_MAPSEC	5

- **MAPsec Transform Identifier** defines at least one mandatory transform used to provide data confidentiality.

Transform ID	Value
RESERVED	0
MAPSEC_AES	1

The following attributes are needed

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

7.2.1.4 MAPsec Security Association Attributes

The following attributes are needed

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

7.2.1.5 MAPsec Payload Contents

Defining different MAPsec payloads is outside the scope of this document. At least the following payloads require modifications or a redefinition:

- Security association payload
- Identification payload

7.2.1.6 MAPsec Key Exchange Requirements

MAPsec DoI does not introduce additional key exchange types.

7.2.2 MAPsec required modifications to standard IKE

In Phase 1 there are no changes to main mode.

A new Phase 2 mode - the MAP mode, must be introduced. The MAP mode differs from the existing IKE quick mode in the following respects:

- Payloads included to the messages of MAP mode are the same as in Quick Mode but the contents of the payloads differ in the case SA payload and ID payloads.
- Either the identity is never sent or if sent it will be the PLMDID in `fqdn` or `der_gn` encoded form (or the `key_id`).

KEYMAT for MAPsec SA template (as in the present Quick mode).

7.2.3 Policy requirements for the MAPsec SPD

The policy is described as in the RFC-2401 [13] 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 MAP SA's are negotiated.

The security policies for MAPsec key management are specified in the KACs' SPD by the network operator. 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.

7.2.4 MAPsec SA transport protocol for the Ze-interface

The stage-3 description for MAPsec SA transport protocol is defined in [some ref] .

Two different modes are defined for this interface:

- The PUSH mode where the MAP-NE subscribes to the MAPsec SA from a particular security domain
- The PULL mode where the MAP-NE explicitly requests a MAPsec SA from a particular security domain

7.2.4.1 MAPsec SA PUSH procedure

The MAPsec SA PUSH procedure is used when the MAP-NE has substantial and frequent traffic towards a security domain. In case like this it makes sense to automatically receive an updated MAPsec SA when the old one is about to expire. The KAC will automatically re-negotiate the SAs.

Two procedures are defined for managing the MAPsec SA subscriptions. Own addresses will be part of the addressing of the requests.

Figure 3: SubscibeSA procedure

A subscription is valid until it is cancelled by the *UnsubscibeSA* procedure. A subscription is valid for exactly one security domain. The MAP-NE may have as many active subscriptions as needed.

Figure 4: UnSubscribeSA procedure

The *UnsubscribeSA* procedure cancels exactly one SA subscription. An invocation of the *UnsubscribeSA* procedure without the a preceding *SubscriptionSA* is invalid and shall be ignored by the KAC.

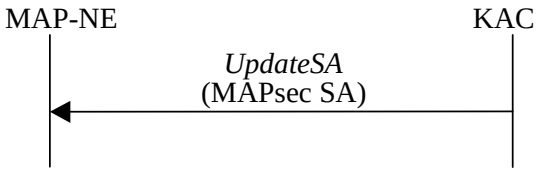


Figure 5: UpdateSA procedure

The *UpdateSA* procedure is executed whenever a subscribed to MAPsec SA is renegotiated by the KAC. The *UpdateSA* procedure then transfers the fresh MAPsec SA from the KAC to the MAP-NE and the new MAPsec SA is then used for all subsequent dialogues from the MAP-NE towards other MAP-NEs in the security domain indicated by the MAPsec SA.

7.2.4.2 MAPsec SA PULL procedure

The MAPsec SA PULL procedure is used when the MAP-NE need close control of the MAPsec SA updating or when the amount of traffic towards a security domain is infrequent.

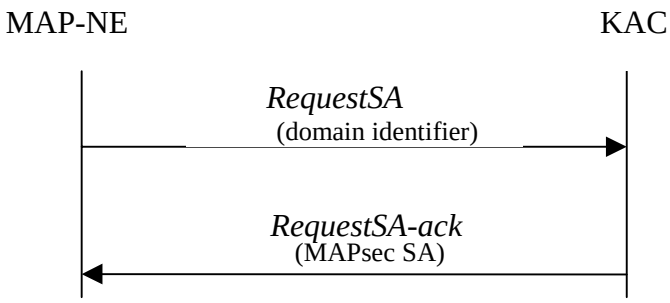


Figure 6: RequestSA procedure

In case like this the MAP-NE only request an SA when it is actually needed or when the MAP-NE detects that the SA is about to expire. When receiving the request the KAC will either directly provide the MAP-NE with an already present SA or it will negotiate an SA with the external security domain before proceeding to return the SA to the MAP-NE.

7.2.5 MAPsec structure of protected operations

7.2.5.1 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 operations 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 operation . 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 operation in cleartext 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 operation.

[EDITOR: I got the impression that a container operation "SecureTransport" is being specified and that it would take a protected operations as its payload. This is not yet reflected in the most current version of TR 33.800 and the the material here may not be completely up to date. This affects 7.2.5.2-5.

Input from companies with CN4 delegates is wanted.]

7.2.5.2 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the protected payload in protection mode 0 is functionally and security wise identical to the original MAP operation payload in cleartext.

For cases where Protection Mode 0 is to be used the protection level will be identical to the original unprotected MAP operation. It is therefore allowed as an implementation option to let Protection Mode 0 operations be sent without the security header.

7.2.5.3 Protection Mode 1

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

TVP||Cleartext|| $H_{KSXY(int)}$(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 session key KS_{XY}(int) 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 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 must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

7.2.5.4 Protection Mode 2

The Secured MAP Message Body in protection mode 2 takes the following form:

$$TVP \| E_{KSXY(con)}(\text{Cleartext}) \| H_{KSXY(int)}(TVP \| \text{MAP Header} \| \text{Security Header} \| E_{KSXY(con)}(\text{Cleartext}))$$

where "Cleartext" is the original MAP message in clear text. Message confidentiality is achieved by encrypting Cleartext with the confidentiality session key KS_{XY}(con). Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and $E_{KSXY(con)}$(Cleartext).

The TVP used for replay protection of Secured MAP messages is a 32 bit time-stamp. The receiving network entity will 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.

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

7.2.6 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.

- **Initialization Vector (IV):**

  Initialization 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 issue is discussed in more detail in RFC 2406. IV has only local significance in the NE.

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

- **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).

7.2.7 MAPsec protection profiles

MAPsec specifies a set of protection profiles. These profiles specifies the required protection level pr MAP operation. The protection profile is then a set of attribute pairs (operation, protection level). Annex B.1 contains definitions for standard MAPsec protection profiles.

Table 3: Example of (Operation, Protection level) attribute pairs

MAP Operation	Protection Mode
SendAuthenticationInfo	2 (authenticity/integrity and confidentiality)
AuthenticationFailureReport	1 (authenticity/integrity)
CheckImei	1 (authenticity/integrity)

The protection level for a specified operation applies for the operation irrespective of the dialogue/application context that the operation is part of. Corollary, a dialogue/application context may contain operations with different protection level.

NOTE: Operations shall have the same protection level for both the request and the response phase.

7.2.8 MAPsec algorithms

Similarly to the case of identification of encryption and integrity algorithms in the access network there is a need for having more than one algorithm to choose from. 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 4: MAPsec Integrity Algorithm identifiers

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

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

Table 5: MAPsec Encryption Algorithm identifiers

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

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

[EDITOR: We need to make a clear distinction here: What goes into the MAPsec DoI RFC and what should remain in the TS. To have the same data both places seems undesirable.]

Annex A (normative): Usage and support of IPsec in the UMTS network domain control plane

NOTE: This is a placeholder for the Rel5 version of the specification.

Annex B (normative): UMTS Security Profiles

The security profiles are partially standardised security associations. That is, a limited set of available security association options is negotiable with the scope of the UMTS network domain security architecture. The security profiles defines ~~the~~ both the negotiable and the non-negotiable parts of UMTS security associations.

The security associations comes in two distinctive variants:

- Security Associations for use with IPsec
- Security Associations for use with MAPsec

For each native IP-based protocol, profiles for the use of IPsec are specified. These may differ for different interfaces or may be identical. A security profile is a selection of options for the use of IPsec in the UMTS core network. When defining security policies and security associations for the use of IPsec, the options selected in the security profile shall be used, thus reducing the IPsec configurations which need to be supported by the UMTS core network. A security profile need not completely determine the choice of security policies and security associations.

A security profile contains following items:

- Security features: integrity/message authentication w/anti-replay protection shall always be used. Confidentiality is optional
- Security protocol: ESP shall always be used.
- Mode: tunnel mode shall always be used.
- Security mechanisms: a set of cryptographic algorithms which must be supported
- Selectors: the selectors which shall be used for security associations
- Support for SA lifetime handling
- Combination of security associations (if applicable)
- Failure handling

B.1 UMTS Security Profile for MAP

B.2 UMTS Security Profile for GTP

Annex C (informative): Change history

It is usual to include an annex (usually the final annex of the document) for specifications under TSG change control which details the change history of the specification using a table as follows:

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

3GPP TS 33.200 V0.4.0 (2001-04)

Technical Specification

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

Keywords
Security, Core Network, 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 the SS7 networks has been identified as potential security risk in 2G systems . Since originally the SS7 networks were the provinces of a small number of large institutions, this was perceived not to be a serious security problem.. This is no longer the case, therefore the need for security considerations has been identified as a high priority item for 3GPP networks. Another significant development has been the introduction of IP as the network layer in the GPRS backbone network and then later in the UMTS network domain, i.e., IP protocol is used for signalling traffic as well as for user traffic. Therefore, the introduction of IP signifies not only a shift towards packet switching, which is a major change by its own accounts, but also a shift towards completely open and easily accessible protocols. The implication is that, from a security point of view, a whole new set of threats and risks must be addressed.

Protecting the core network signalling protocols, i.e., security solutions for both SS7 and IP based protocols, is a clear architectural requirement for a 3G system.

Various protocols and interfaces are used to control the signalling plane,, inter as well as intra core network. The following security services have been identified as essential: confidentiality, integrity, authentication and anti-replay protection. The security services will be standardized, based on industry acceptable cryptographic techniques.

1 Scope

This document defines the security architecture for the UMTS network domain control plane. The scope of the UMTS network domain control plane includes the control signalling in the UMTS core network., both the SS7 as well as the IP based control plane signalling protocols.

The UMTS core network contains a number of SS7 based protocols, which are referred to as “legacy protocols” in this specification document. While the stated goal of the network domain security is to cover all core network protocols, not all legacy protocols will be protected in Rel4 timeframe. This decission has been made due to practical technical and commercial constraints, i.e., the SS7 legacy protocols can realistically be protected only at the application layer. Protecting the SS7 network at a lower layer will require large development efforts, including the redesign of the current SS7 protocol itself. Even if this development is technically feasible, it is questionable whether the commercial benefits can ever justify the required development effort. Therefore, the only “legacy protocol” that shall be protected in Rel4 is the MAP protocol [4].

NOTE-1: Lawful Interception considerations and requirements are covered in separate specifications [8,9].

NOTE-2: 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 33.106: Lawful interception requirements

[9] 3G TS 33.107: Lawful interception architecture and functions

[10] 3G TS 33.120: Security Objectives and Principles

[11] 3G TR 33.800: Principles for Network Domain Security

[12] RFC-2393: IP Payload Compression Protocol (IPComp)

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

[14] RFC-2402: IP Authentication Header

[15] RFC-2403: The Use of HMAC-MD5-96 within ESP and AH

[16] RFC-2404: The Use of HMAC-SHA-1-96 within ESP and AH

[17] RFC-2405: The ESP DES-CBC Cipher Algorithm With Explicit IV

[18] RFC-2406: IP Encapsulating Security Payload

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

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

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

[22] RFC-2410: The NULL Encryption Algorithm and Its Use With IPsec

[23] RFC-2411: IP Security Document Roadmap

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

[25] RFC-2451: The ESP CBC-Mode Cipher Algorithms

[26] RFC-2521: ICMP Security Failures Messages

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

[28] ITU-T

[29] ITU-T

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 goal is to protect against an authorized retransmission of a captured data unit The data unit may have been validated via a cryptographical integrity mechanism.

Data confidentiality: The property that the data flow is protected from disclosure to an unauthorised individuals, entities or processes. Data confidentiality is supported by encryptions algorithms that convert a plain text message into an encrypted message (or ciphertext).

Data integrity: The property that ensures that messages are received as sent, with no duplication, insertion, modification, reordering or replay.. Data integrity is provided by calculating a cryptographic (e.g., Keyed Hashing) message digest (called Message Authentication Code or MAC) based on the message content. Any changes in the message content will trigger a corresponding change in the message MAC.

Data origin authentication: The corroboration that the message is from the source that is claims to be from.

Entity authentication: The provision of assurance of the claimed identity of an entity.

IPSec SA: provide security services at the IP layer and is enabling a system to select required security protocols: Authentication Header (AH) or Encapsulation Security Protocol (ESP), determine the algorithms to be used, the transforms, the keys, and the duration for which the keys are valid. The IPSec is stored in a SA Database (SADB), it is protocol specific and unidirectional. If a pear relationship is needed, then two security associations are required:

- **Security Parameter Index (SPI)** A bit string assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- **IP Destination Address** : the address of the destination endpoint of the SA (e.g., end user, or network entity).
- **Security Protocol Identifier**: indicates whether the association is an AH or ESP security association.

Key freshness: A key is fresh if it can be guaranteed to be new (i.e., the key shall not be reused through actions of either an adversary or authorised party).

Legacy protocols: Network utilizing SS7 or mixed SS7/IP based protocols will be commonly referred to as" within this document

MAP: TCAP carries **Mobile Application Part** (MAP) messages sent between mobile switches and databases to support user authentication, equipment identification, and roaming.

Security Association (SA): A one-way relationship between the sender and the receiver that ensures the security of the traffic carried on.. All traffic traversing a SA is protected by the same security protocol.

SS7: Common Channel Signalling System #7 (SS7) is a global telecommunications standard (defined by ITU-T) for the signalling system that allows the various components of a telephone network to exchange information and connect calls. Used in both wireless and wireline networks

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
F	MAP interface between a MSC and an EIR
Gc	Interface between a GGSN and an HLR
Gd	Interface between an MSC and an SGSN
Gf	Interface between an SGSN and an EIR
Gi	Reference point between GPRS and an external packet data network
Gn	Interface between two GSNs within the same PLMN
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs
Gr	Interface between an SGSN and an HLR
Gs	Interface between an SGSN and an MSC/VLR.
Iu	Interface between the RNS and the core network. It is also considered as a reference point.
Iur	Interface between RNSs in the access network
Za	Interface between SEGs belonging to different networks/security domains
Zb	Interface between SEGs and NEs within the same network/security domain
Zc	Interface between NEs within the same network/security domain
Zd	Interface between KACs belonging to different networks/security domains
Ze	Interface between KACs and MAP-NEs within the same network
Zf	Interface between networks/security domains for secure interoperation. MAP-NE ←→MAP-NE.

3.3 Abbreviations

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

AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
BG	Border Gateway
CS	Circuit Switched
DES	Data Encryption Standard
DoI	Domain of Interpretation
ESP	Encapsulating Security Payload
GTP	GPRS Tunnelling Protocols
IESG	Internet Engineering Steering Group
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
NAT	Network Address Translator
NDS	Network Domain Security
NE	Network Entity
PS	Packet Switched
RNS	Radio Network Subsystem
SA	Security Association
SAD/SADB	Security Association Database (sometimes also referred to as SADB)
SEG	Security Gateway
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
SS7	`Signalling System no. 7 protocol
TVP	Time Variant Parameter
USP	UMTS Security Profile

4 Overview over UMTS network domain security

4.1 Introduction

The scope of this section is to outline the basic principles for the network domain security architecture. A central concept introduced in this specification is the notion of a network security domain. A security domain is a network with its security managed by a single administrative authority. Within a security domain, the same level of security, as well as the same usage of the security services, is supported. Typically, a network operated by a single operator will support one security domain, although an operator may subdivide it's network into separate sub-networks and hence creating multiple security domains.

In this specification, a distinction is made between protocols using SS7 based networks and IP based networks as their transport mechanism. Ideally no such distinction should have had to be made, but technical differences between the SS7 and IP architectures have forced the following high-level sub-sectioning:

- **If native IP based networks are to be protected, they shall be protected at the network level by means of the IPsec protocols**

  The UMTS network domain control plane is subdivided into multiplesecurity domains. Typically those domain align with an operator's service area borders. The border between the security domains is protected by Security Gateways (SEGs). The SEG is responsible for enforcing the security policy of it's own security domain in relationship to all other SEG associated with the destination security domain. The network operator may have multiple SEGs in its network in order to avoid a single point of failure (i.e., redundancy) or for performance reasons (e.g., distributed processing). One SEG may be associated with all reachable security domain destinations or it may be defined for only a subset of the reachable destinations.

  The UMTS network domain security does not extend to the user plane and consequently the security domains and the associated security gateways towards other domains do no encompass the user plane Gi interface .

- **If a networks using SS7 protocol is to be protected, it shall be protected at the Mobile Application Part (MAP) level**

  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 be commonly referred to as "legacy protocols" within this document.

  For legacy protocols, the necessary security associations (SA) between networks are negotiated between Key Administration Centre (KAC) entities. The negotiated SA will be enforced network-wide and distributed to all relevant network elements. For routing purposes, the signalling traffic, which is protected at the application

layer, , will be indistinguishable from unprotected traffic to all intermediate nodes, except for the sending and receiving entities. In order to avoid a single point of failure or for performance reasons, a network operator may have more than one KAC in his/her network. A KAC may be assigned to control the security interaction among all the reachable security domain destinations or it may be defined for only a subset of the reachable domain destinations.

NOTE-1: It is explicitly noted that protection for IP based protocols is not part of Rel4. Protection for IP based protocols is targeted for Rel5 of this technical specification.

NOTE-2: 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.

4.2 Security for SS7 and mixed SS7/IP based protocols

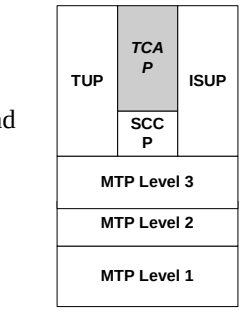
Legacy protocols shall be protected at the application layer (i.e., MAP layer). This requires changes to the application protocols themselves to provide the necessary security functionality. This document contains the stage-2 specification required to provide security protection to the legacy protocols. The actual implementation (stage-3) specification can be found in the specification associated with the target protocol.

Overview over security protected SS7 based protocols for Rel4:

- **Mobile Application Part** (MAP)

  ecurity for MAP messages (carried within TCAP messages) shall be provided by the MAP security protocol. The MAP security protocol stage-2 specification can be found in section 7 and Annex B.1 and the stage-3 specifications can be found in TS 29.002 [4].

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



SS7 Protocol Stack

4.3 Security for native IP based protocols

NOTE: This is a placeholder for the Rel5 version of the specification.

4.4 Security domains

4.4.1 Security domains and interfaces

The UMTS network domain shall be logically and physically divided into security domains. The control plane security domains, which may closely correspond to the core network of a single operator, may interface with other control plane domains via security gateways (SEG).

The specific network domain security interfaces is found in table 1. Section 5.2 contains a detailed description of the Z-interfaces.

Table 1: Network domain security specific interfaces

Interface	Description	Network type
Za	Network domain security interface between SEGs. The interface is used for both the negotiation of security associations and for the set-up of ESP protected tunnels between SEGs (no third party negotiation).	IP
Zb	Network domain security interface between SEGs and NEs within the same network. The interface is used for both the negotiation of security associations and for the set-up of an ESP protected tunnel.	IP
Zc	Network domain security interface between NEs within the same network. The interface is used for both the negotiation of security associations and for the set-up of an ESP protected tunnel.	IP
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/is affected by the network domain security 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 remaining interfaces only applies to Rel5, but is included here for information.

Table 2: Interfaces that are affected by network domain 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
F	Interface between MSC and EIR	MAP	MAPsec shall be supported
G	Interface between VLR and VLR	MAP	MAPsec shall be supported
J	Interface between HLR and gsmSCF	MAP	MAPsec shall be supported
Gc	Optional interface between GGSN and HLR	MAP	MAPsec shall be supported
Gd	Interface between SMS-MSCs and SGSN	MAP	MAPsec shall be supported
Gf	Interface between SGSN and EIR	MAP	MAPsec shall be supported
Gn	Interface between GSNs within the same network	GTP	ESP shall be supported
Gp	Interface between GSNs in different PLMNs.	GTP	IPsec shall be supported. Security Gateways shall be present at the domain borders.
Gr	Interface between SGSN and HLR	MAP	MAPsec shall be supported

NOTE-1: The requirement for MAPsec support is dependent on the MAPsec security profile.

NOTE-2: The Iu and Gs interfaces are presently not covered by NDS.

NOTE-3: It is explicitly noted that only the MAP interfaces are covered by Rel4. Coverage for the GTP interfaces will be introduced with Rel5 of this specification.

4.5 Security Gateways (SEGs)

NOTE: This is a placeholder for the Rel5 version of the specification.

4.6 Key Administration Centres (KACs)

Key Administration Centres (KACs) are network entities negotiating MAPsec SAs on behalf of MAP-NEs. The KACs are defined to support secure communication over the:

- the Zd-interface between KACs associated with different MAP security domains. Internet Key Exchange (IKE) protocol with support for MAPsec DoI shall be used over this interface.

- the Ze-interface between a KAC and a MAP-NE within the same MAP security domain is used to transfer MAPsec SAs from KACs to MAP-NEs. IKE and the ESP protocols may be used to negotiate and secure the connection between the KAC and the MAP-NE.

When a MAP-NE needs to establish a secure connection with another MAP-NE it will request a MAPsec SA from the KAC. The KAC will then either provide an existing MAPsec SAs or negotiate a new MAPsec SA, before returning the MAPsec SA to the MAP-NE.

A MAPsec SA is valid for all MAP communication between the two security domains for which it was negotiated. That is, the same MAPsec SA shall be provided to all MAP-NE in the same security domain (e.g., domain A) when communication with the MAP-NEs in a different security domain (e.g., domain B). Each security domain may have one or more KACs. Each KAC will control the MAPsec SAs associated with a pre-defined set of reachable MAP security domains. The number of different KACs in a specific security domain depends on the need to differentiate between the externally reachable destinations, the need to balance the traffic load and the need to avoid a single point of failures.

The following are the most important tasks for a KAC:

- Perform MAP-SA negotiation with KACs belonging to other security domains. This action is triggered either by a NE's request for a MAP-SA or by a security policy enforcement directive.

- Perform refresh of a MAP-SA. The refresh can be triggered internally by the MAP-SA lifetime supervision, based on the policies set by an operator and established during the negotiation protocol.

- Distribute valid MAP-SAs to requesting nodes that belong to the same network as the KAC. This is done according to the MAP-SA transport procedures defined in section 7.2.4.

- Establish ESP protected communication between itself and all other NEs in its own network

More information on KACs can be found in 5.3 and section 7.

KACs are responsible for managing and controlling security sensitive operations and shall be physically secured. They shall also offer capabilities for the secure storage of long-term keys used for IKE authentication.

NOTE: It is explicitly noted that Key Administration Centres are not part of Rel4 of MAPsec. Consequently, there is not requirement for a KAC in a Rel4 network.. KACs will be introduced in Rel5 of this specification and this section is only for information.

5 Key management and distribution architecture for the UMTS core network

5.1 Security Associations (SAs)

NOTE: This is a placeholder for the Rel5 version of the specification.

5.2 Use of the Internet Key Exchange protocol

NOTE: This is a placeholder for the Rel5 version of the specification.

5.3 UMTS key management and distribution architecture for native IP based protocols

NOTE: This is a placeholder for the Rel5 version of the specification.

5.4 UMTS key management and distribution architecture for SS7 and mixed SS7/IP-based protocols

The following section specifies the generic parts of the key management and distribution architecture for SS7 and mixed SS7/IP-based protocols. Since the security mechanisms is implemented at the application layer, a number of the issues are unique to this implementation. Section 7 contains detailed and specific requirements for the applicable application protocols.

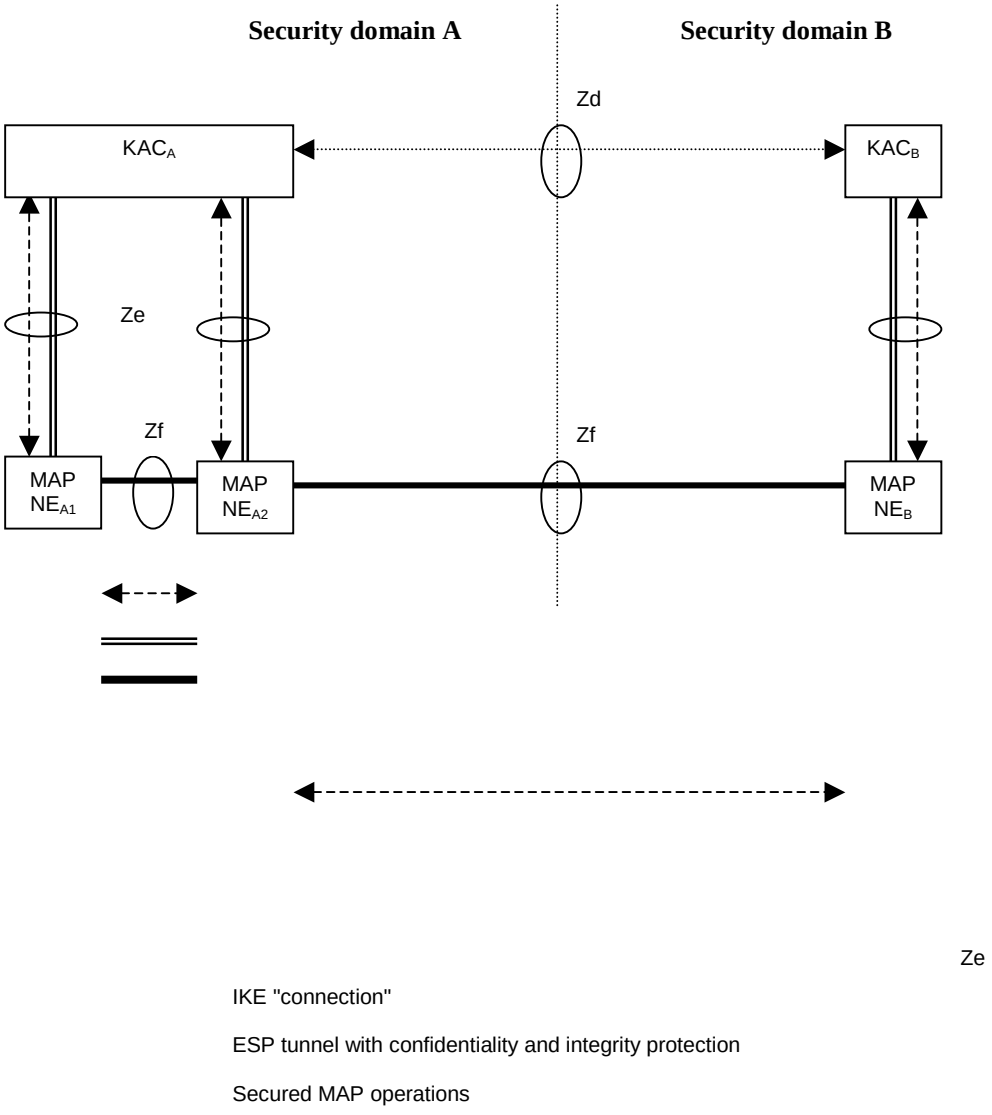


Figure 2: Overview of the Zd, Ze and Zf interfaces

Only SS7 MAP protocol shall be protected in Rel4. . References to MAP security (MAPsec) may be expended to be more generic in later releases.

The following interfaces are defined MAPsec.

- **Zd-interface (KAC-KAC)**

  The Z-d-interface is used to negotiate MAPsec Security Associations (SAs) between MAP security domains. The traffic over Zd consists only of IKE negotiations. The negotiated MAPsec SAs are valid only between two specific security domain.

- **Ze-interface (KAC-NE)**

The Ze-interface is between MAP-NEs and a KAC within the same MAP security domain. The KAC and the MAP-NE are capable of establishing and maintaining an ESP tunnel between them. Whether the tunnel is established when needed or a priori is for the MAP security domain operator to decide. The tunnel is subsequently used for transporting MAPsec SAs from the KAC to the target MAP-NE.

- **The Zf-interface (NE-NE)**

  The Zf-interface is between MAP-NEs. The MAP-NEs may belong to the same security domain or to different security domains (as shown in figure 2). The MAP-NEs use MAPsec SAs received from a KAC to protect the MAP operations. The MAP operations within the MAP dialogue are selectively protected, as specified in the applied MAPsec security profile.

NOTE: It is explicitly noted that there is no Rel4 requirements for support of KACs or the associated Zd/Ze-interfaces. KACs and its associated interfaces and protocols will only be introduced in Rel5. For Rel4 this section is only for information.

6 Security for native IP based protocols

NOTE: This is a placeholder for the Rel5 version of the specification.

7 Security for SS7 and mixed SS7/IP based protocols

7.1 Security services afforded to the protocols

The security services required for SS7 and mixed SS7/IP-based protocols are:

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

7.2 MAP security (MAPsec)

This section describes mechanisms for establishing secure signalling links between MAP network entities

7.2.1 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 shall be defined and published within the IETF framework as a separate RFC ([27]. Since the MAPsec DoI RFC addresses only non-IP issues, it will be an informational RFC, but it shall nevertheless be normative for UMTS MAPsec purposes.

7.2.1.1 MAPsec DoI requirements

ISAKMP (RFC-2408, [20]) 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

IANA will not normally assign a DoI value without referencing some public specification, such as an Internet RFC. Without a DoI value assigned by IANA, the MAP SA negotiation over the interface Z_D is not possible. MAPsec DoI for ISAKMP draft *must* be written, since the new DoI is an essential part of the key management architecture.

The following sections define briefly the requirements for MAPsec DoI for ISAKMP.

7.2.1.2 MAPsec Situation definition

Within ISAKMP, the Situation provides information that the responder can use to determine how to process incoming SA request. For the MAPcec DoI, the Situation field is always left empty.

7.2.1.3 MAPsec Security Policy Requirements

The MAPsec DoI does not impose specific security policy requirements on any implementation.

MAPSec Assigned Numbers

The following sections list the Assigned Numbers for the MAPsec DoI: protocol identifiers and transform identifiers.

- **MAPsec Protocol Identifier** defines a value for the Security Protocol Identifier referenced in an ISAKMP Proposal Payload for the MAPsec DoI.

Protocol ID	Value
PROTO_MAPSEC	5

- **MAPsec Transform Identifier** defines at least one mandatory transform used to provide data confidentiality.

Transform ID	Value
RESERVED	0
MAPSEC_AES	1

The following attributes are needed

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

7.2.1.4 MAPsec Security Association Attributes

The following attributes are needed

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

7.2.1.5 MAPsec Payload Contents

Defining different MAPsec payloads is outside the scope of this document. At least the following payloads require modifications or a redefinition:

- Security association payload
- Identification payload

7.2.1.6 MAPsec Key Exchange Requirements

MAPsec DoI does not introduce additional key exchange types.

7.2.2 MAPsec required modifications to standard IKE

In Phase 1 there are no changes to main mode.

A new Phase 2 mode - the MAP mode, must be introduced. The MAP mode differs from the existing IKE quick mode in the following respects:

- Payloads included to the messages of MAP mode are the same as in Quick Mode but the contents of the payloads differ in the case SA payload and ID payloads.
- Either the identity is never sent or if sent it will be the PLMDID in `fqdn` or `der_gn` encoded form (or the `key_id`).

KEYMAT for MAPsec SA template (as in the present Quick mode).

7.2.3 Policy requirements for the MAPsec SPD

The policy is described as in the RFC-2401 [13] 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 MAP SA's are negotiated.

The security policies for MAPsec key management are specified in the KACs' SPD by the network operator. 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.

7.2.4 MAPsec SA transport protocol for the Ze-interface

The stage-3 description for MAPsec SA transport protocol is defined in [some ref] .

Two different modes are defined for this interface:

- The PUSH mode where the MAP-NE subscribes to the MAPsec SA from a particular security domain
- The PULL mode where the MAP-NE explicitly requests a MAPsec SA from a particular security domain

7.2.4.1 MAPsec SA PUSH procedure

The MAPsec SA PUSH procedure is used when the MAP-NE has substantial and frequent traffic towards a security domain. In case like this it makes sense to automatically receive an updated MAPsec SA when the old one is about to expire. The KAC will automatically re-negotiate the SAs.

Two procedures are defined for managing the MAPsec SA subscriptions. Own addresses will be part of the addressing of the requests.

Figure 3: SubscibeSA procedure

A subscription is valid until it is cancelled by the *UnsubscibeSA* procedure. A subscription is valid for exactly one security domain. The MAP-NE may have as many active subscriptions as needed.

Figure 4: UnSubscribeSA procedure

The *UnsubscribeSA* procedure cancels exactly one SA subscription. An invocation of the *UnsubscribeSA* procedure without the a preceding *SubscriptionSA* is invalid and shall be ignored by the KAC.

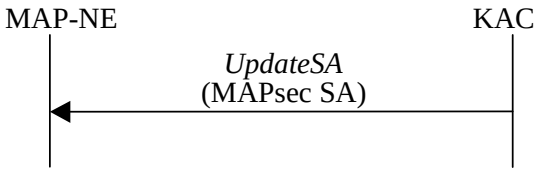


Figure 5: UpdateSA procedure

The *UpdateSA* procedure is executed whenever a subscribed to MAPsec SA is renegotiated by the KAC. The *UpdateSA* procedure then transfers the fresh MAPsec SA from the KAC to the MAP-NE and the new MAPsec SA is then used for all subsequent dialogues from the MAP-NE towards other MAP-NEs in the security domain indicated by the MAPsec SA.

7.2.4.2 MAPsec SA PULL procedure

The MAPsec SA PULL procedure is used when the MAP-NE need close control of the MAPsec SA updating or when the amount of traffic towards a security domain is infrequent.

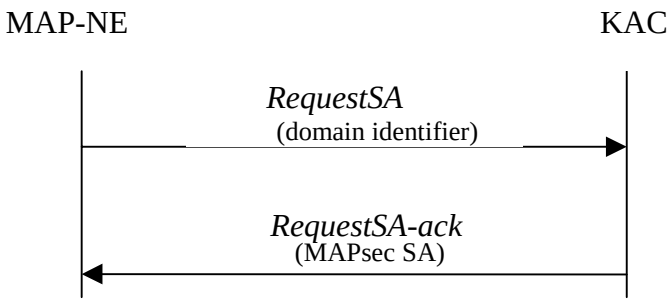


Figure 6: RequestSA procedure

In case like this the MAP-NE only request an SA when it is actually needed or when the MAP-NE detects that the SA is about to expire. When receiving the request the KAC will either directly provide the MAP-NE with an already present SA or it will negotiate an SA with the external security domain before proceeding to return the SA to the MAP-NE.

7.2.5 MAPsec structure of protected operations

7.2.5.1 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 operations 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 operation . 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 operation in cleartext 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 operation.

[EDITOR: I got the impression that a container operation "SecureTransport" is being specified and that it would take a protected operations as its payload. This is not yet reflected in the most current version of TR 33.800 and the the material here may not be completely up to date. This affects 7.2.5.2-5.

Input from companies with CN4 delegates is wanted.]

7.2.5.2 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the protected payload in protection mode 0 is functionally and security wise identical to the original MAP operation payload in cleartext.

For cases where Protection Mode 0 is to be used the protection level will be identical to the original unprotected MAP operation. It is therefore allowed as an implementation option to let Protection Mode 0 operations be sent without the security header.

7.2.5.3 Protection Mode 1

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

TVP||Cleartext|| $H_{KSXY(int)}$(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 session key KS_{XY}(int) 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 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 must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

7.2.5.4 Protection Mode 2

The Secured MAP Message Body in protection mode 2 takes the following form:

$$TVP \| E_{KSXY(con)}(\text{Cleartext}) \| H_{KSXY(int)}(TVP \| \text{MAP Header} \| \text{Security Header} \| E_{KSXY(con)}(\text{Cleartext}))$$

where "Cleartext" is the original MAP message in clear text. Message confidentiality is achieved by encrypting Cleartext with the confidentiality session key KS_{XY}(con). Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and $E_{KSXY(con)}$(Cleartext).

The TVP used for replay protection of Secured MAP messages is a 32 bit time-stamp. The receiving network entity will 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.

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

7.2.6 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.

- **Initialization Vector (IV):**

  Initialization 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 issue is discussed in more detail in RFC 2406. IV has only local significance in the NE.

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

- **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).

7.2.7 MAPsec protection profiles

MAPsec specifies a set of protection profiles. These profiles specifies the required protection level pr MAP operation. The protection profile is then a set of attribute pairs (operation, protection level). Annex B.1 contains definitions for standard MAPsec protection profiles.

Table 3: Example of (Operation, Protection level) attribute pairs

MAP Operation	Protection Mode
SendAuthenticationInfo	2 (authenticity/integrity and confidentiality)
AuthenticationFailureReport	1 (authenticity/integrity)
CheckImei	1 (authenticity/integrity)

The protection level for a specified operation applies for the operation irrespective of the dialogue/application context that the operation is part of. Corollary, a dialogue/application context may contain operations with different protection level.

NOTE: Operations shall have the same protection level for both the request and the response phase.

7.2.8 MAPsec algorithms

Similarly to the case of identification of encryption and integrity algorithms in the access network there is a need for having more than one algorithm to choose from. 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 4: MAPsec Integrity Algorithm identifiers

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

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

Table 5: MAPsec Encryption Algorithm identifiers

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

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

[EDITOR: We need to make a clear distinction here: What goes into the MAPsec DoI RFC and what should remain in the TS. To have the same data both places seems undesirable.]

Annex A (normative): Usage and support of IPsec in the UMTS network domain control plane

NOTE: This is a placeholder for the Rel5 version of the specification.

Annex B (normative): UMTS Security Profiles

The security profiles are partially standardised security associations. That is, a limited set of available security association options is negotiable with the scope of the UMTS network domain security architecture. The security profiles defines both the negotiable and the non-negotiable parts of UMTS security associations.

The security associations comes in two distinctive variants:

- Security Associations for use with IPsec
- Security Associations for use with MAPsec

For each native IP-based protocol, profiles for the use of IPsec are specified. These may differ for different interfaces or may be identical. A security profile is a selection of options for the use of IPsec in the UMTS core network. When defining security policies and security associations for the use of IPsec, the options selected in the security profile shall be used, thus reducing the IPsec configurations which need to be supported by the UMTS core network. A security profile need not completely determine the choice of security policies and security associations.

A security profile contains following items:

- Security features: integrity/message authentication w/anti-replay protection shall always be used. Confidentiality is optional
- Security protocol: ESP shall always be used.
- Mode: tunnel mode shall always be used.
- Security mechanisms: a set of cryptographic algorithms which must be supported
- Selectors: the selectors which shall be used for security associations
- Support for SA lifetime handling
- Combination of security associations (if applicable)
- Failure handling

B.1 UMTS Security Profile for MAP

B.2 UMTS Security Profile for GTP

Annex C (informative): Change history

It is usual to include an annex (usually the final annex of the document) for specifications under TSG change control which details the change history of the specification using a table as follows:

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

3GPP TSG SA WG3 Security — S3#17bis **S3-010xxx**
23rd April – 24th April
Madrid, Spain

CR-Form-v3

CHANGE REQUEST

⌘ **33.200** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **0.4.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Editorial changes to the requirements document
Source:	⌘	Lucent Technologies
Work item code:	⌘	Network Domain Security
Date:	⌘	23-April-01
Category:	⌘	**D**
Release:	⌘	

Use one of the following categories:
F *(essential correction)*
A *(corresponds to a correction in an earlier release)*
B *(Addition of feature),*
C *(Functional modification of feature)*
D *(Editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	Clarify the text, add new definitions
Summary of change:	⌘	Multiple editorial changes
Consequences if not approved:	⌘	Document may not be clear

Clauses affected:	⌘	1 - 7.2.1
Other specs Affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	