S3-010026

3GPP TS 33.200 V0.3.1 (2001-01)

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

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 province of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions. 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. Furthermore, IP is not only used for signalling traffic, but also for user traffic. The 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.

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. These include among the protocols MAP and GTP, among the interfaces Iu and Iur, and possibly other protocols or interfaces that are new to R4 or have yet to be identified. 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.

Perhaps the most crucial element of a sound security architecture is the key management and distribution component. Significant effort has been put into establishing a key management and distribution architecture that can be applied to both SS7 and IP based protocols, while still remain sufficiently simple as to ensure ease of implementation and reliable interworking.

1 Scope

The present document defines the security architecture for the UMTS network domain control plane. The scope of the UMTS network domain control plane is to cover the control signalling in the UMTS core network with extension to cover the Iu-interface towards RNS. This includes both the SS7 and IP based control plane signalling protocols.

The UMTS core network contains a number of SS7 based protocols, which in this specification is referred to as legacy protocols. 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 R4. 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 where 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 R4 is the MAP protocol [4]. Protection of the Iu/Iur-interfaces is not considered part of R4.

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

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 TR 29.002: Mobile Application Part (MAP) specification

[5] 3G TR 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 TS 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

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 cryptography integrity mechanism in place. Anti-replay protection is particularly important when data origin authentication is also used for the purpose of entity authentication.

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 group of parameters to define an IPsec protocol for a one-way security protection between two entities. A Security Association includes the cryptographic algorithms, the keys, the duration of the keys, and other parameters.

Transport mode: A mode of operation for IPsec protocol. It protects the payload of the IP packet, in effect giving protection to higher level layers.

Tunnel mode: A mode of operation for IPsec protocol. It protects the IP packet payload and the header. By tunnel mode, a packet may be tunnelled from one point to another. The endpoints may be different from the original resource and destination of the protected IP packet.

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 security domains
Zb	Interface between a SEG and a NE or between NEs within the same security domain
Zc	Interface between KACs belonging to different security domains in native IP networks
Zd	Interface between KACs and NEs or SEGs within the same network
Ze	Interface between KACs in SS7 or SS7/IP mixed network
Zf	Interface between KAC and MAP-NEs in SS7 or SS7/IP mixed network
Zg	Interface between MAP-NEs from different security domains.

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
CS	Circuit Switched
DES	Data Encryption Standard
DoI	Domain of Interpretation
ESP	Encapsulating Security Payload
GTP	GPRS Tunnelling Protocols
IETF	Internet Engineering Task Force
IESG	Internet Engineering Steering Group
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	Initialization Vector
KAC	Key Administration Centre
MAC	Message Authentication Code
MAP	Mobile Application Part
MAPsec	MAP security – the MAP protocol with security enhancements
NAT	Network Address Translator
NDS	Network Domain Security
NE	Network Entity
PS	Packet Switched
RNS	Radio Network Subsystem
SA	Security Association
SAD	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
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 notion of a network security domain. The security domains are networks that from a security point of view are physically and/or logically separated. Within a security domain the same level of security services will be provided. 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.

In this specification a distinction between protocols carried by SS7 and IP based networks are made. Ideally no such distinction should have had to be made, but the technical differences between the SS7 and IP architectures has forced the following high-level sub-sectioning:

- **Native IP based protocols shall be protected at the network level by means of the IPsec protocols**

  The UMTS network domain control plane is also sectioned into security domains and typically these coincide with operator borders. The border between the security domains is protected by Security Gateways (SEGs). The SEGs are responsible for enforcing the security policy of a security domain towards other SEGs in the destination security domain. The network operator may have more than one SEG in its network in order to avoid a single point of failure or for performance reasons. A SEG may be defined for interaction towards all reachable security domain destinations or it may be defined for only a subset of the reachable destinations. It is noted that SEGs and Border Gateways (BG) could be co-located and even implemented within the same physical node.

  Key Administration Centres (KACs) negotiate the inter-domain IPsec Security Associations (SAs) by using Internet Key Exchange (IKE) protocol in client mode on behalf of network entities (NEs) and SEGs in its own security domain. KACs also distribute SAs to NEs or SEGs.

  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.

- **SS7 based protocols are to be protected at the application level**

  As 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.

  The necessary security associations between networks are negotiated by Key Administration Centre entities. The primary purpose of the KACs is to negotiate security associations for use with the SS7 application protocols. 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 to unprotected traffic to all parties except for the sending and receiving sides. 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.

4.2 Security for SS7 and mixed SS7/IP based protocols

Legacy protocols shall be protected at the application layer. This implies changes to the application protocols themselves to allow for the necessary security functionality. This specification shall contain the stage-2 specification for the security protection of the legacy protocols. The actual implementation (stage-3) specification shall be found in the specification for the target protocol.

Overview over security protected SS7 based protocols for R4:

- **Mobile Application Part**

  Security for MAP shall be provided by the MAP security protocol. The MAP security protocol stage-2 specification is found in section 7 and stage-3 specification is found in TS 29.002 [4].

- It is for further study whether other legacy protocols need to be protected in future releases

NOTE: It has been recognized that mixed SS7/IP based protocols may also be protected at the network layer when using IP as the transport protocol. It may indeed be desirable to protect such protocols at the network layer for operators that no longer use the SS7 version of the protocol. For R4 no such case has been identified.

4.3 Security for native IP based protocols

For native IP-based protocols, security shall be provided at the network layer. The security protocols to be used at the network layer is the IPsec security protocols as specified in RFC-2401 [12]. All network entities supporting native IP-based control plane protocols shall support IPsec.

The usage of IPsec in the UMTS network domain control plane shall adhere to the rules and requirements specified in section 6 and Annex A. The main rules and requirements are summarized as follows:

- Use of IPsec payload compression [12] is not supported.
- Support of IPsec ESP [18] is required.
- Support of IPsec tunnel mode is required. When at least one of the endpoints is a Security Gateway (SEG), tunnel mode should be used.
- Support IPsec transport mode is required. When neither of the endpoints is a Security Gateway (SEG), transport mode should be used.
- Anti-replay protection shall always be used.
- ESP shall always be used with authentication on (use of NULL authentication algorithm is not allowed).
- The ESP_DES encryption transform shall not be used.
- All secure communication between security domains takes place through SEGs.
- A chained-tunnel/hub-and-spoke approach is used. That is, all the inter-domain IP packets will be tunnelled from one SEG from its resource domain to another SEG in its destination domain.
- Key management for IPsec shall always be automated in order to support IPsec anti-replay protection.

4.4 Security domains

4.4.1 Security domains and interfaces

The UMTS network domain shall be logically and physically divided into security domains. Each control plane security domain corresponds to the core network of a single operator. Different security domains shall be separated by means of security gateways.

Network Domain Security protocols are defined over interfaces. An interface is usually defined between two parties in the network domain. These interfaces are listed in table 1. Section 5.2 contains a detailed description for the security protocols over each of the interfaces.

Network Domain Security protocols provide security protections over communication interfaces in core networks. Table 2 list all the communication interfaces protected by Network Domain Security protocols.

Table 1: Network domain security specific interfaces

Interface	Description	Affected protocol
Za	Interface between two SEGs in different security domains. The packets crossing the security domains are protected by IPsec ESP protocol in tunnel mode with SEGs as endpoints.	IPsec/ESP
Zb	Interface between a SEG and a NE or between two NEs within the same network. Intra-domain SA may be negotiated over this interface. IPsec ESP can be used to protect the communications over this interface,	Intra-domain IKE and IPsec/ESP
Zc	Interface between two KACs in different security domains. Zc interface is defined for negotiations of Inter-domain SAs. The communications over this interface should be protected by IPsec ESP.	Inter-domain IKE and IPsec ESP
Zd	Interface between a KAC and a NE or a SEG in the same security domain. Intra-domain SA may be negotiated over this interface. KAC may distribute inter-domain SAs to NEs or SEGs via this interface under the protection of IPsec ESP.	Intra-domain IKE and IPsec ESP
Ze	Interface between KACs in different networks. The Ze-interface is defined for negotiation of MAP security associations.	Inter-domain IKE
Zf	Interface between KAC and MAP-NE within the same network. The interface is protected by means of an IPsec ESP tunnel. The transport protocol is HTTP.	IPsec ESP and HTTP
Zg	Interface between MAP-NEs engaged in security protected signalling	MAPsec

The core network interfaces, which affects or are affected by the network domain security specification, are described in the table below.

Table 2: Interfaces that is 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
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	IPsec 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
Gs	Interface between SGSN and VLR/MSC	MAP	MAPsec shall be supported
Iu	Interface between RNS and SGSN/VLR	RANAP	ffs
Iur	Interface between RNSs in the access network	RNSAP	ffs

4.4.2 Security termination points

By a terminating point one here understand a network point where the signalling traffic will be present in clear at some stage. Security protection is terminated in the following entities:

SS7 based protocols:

MAP security is effective end-to-end. The sending and the receiving MAP-NEs will be the terminating points.

Native IP based protocols:

If tunnel mode is used, every end-point of a tunnel must be viewed as a termination point. The only defined tunnel termination points are the communicating entities themselves and possibly one or more SEGs. It is noted that the SEGs are trusted entities.

NOTE: For native IP based protocols, the only termination points must be communicating entities and Security Gateways. Each Security Gateway, if it is a termination point, then it must belong to the same security domain as either of communicating entities. This holds irrespective of the fact that there may be intermediate networks between the communicating entities.

4.4.3 Filtering routers and firewalls

In order to strengthen the security for IP based networks, border gateways and access routers would normally use packet filtering strategies to prevent certain types of traffic to pass in or out of the network. Similarly, firewalls are used as an additional measure to prevent certain types of accesses towards the network.

The rationale behind the application of packet filters and firewalls should be found in the security policy of the network operator. Preferably, the security policy should be an integral part of the network management strategy as a whole.

While network operators are strongly encouraged to use filtering routers and firewalls, the usage, implementation and security policies associated with these are considered outside the scope of this specification.

4.4.5 Network Address Translators (NATs)

Network Address Translators (NATs) are not designed to be part of the UMTS network domain control plane. Indeed, the use of NATs are quite troublesome in conjunction with IPsec since the IPsec security protocols either hides private addresses through encryption and thus let them escape translation or the IPsec security protocols experience integrity violations as a consequence of the NAT manipulating protected IP addresses. Both cases are clearly unwanted and will lead to lost communication.

However, since the shortage of available address space for IPv4 is likely to force operators to use private address spaces, the practical need for NATs is recognized if not endorsed. Given this state of affairs, the UMTS network domain control plane security architecture has been designed to allow for NATs to be present in the networks.

NOTE: The use of NATs are not endorsed by the security specification group and operators are encouraged to avoid the use of NATs if at all possible.

4.5 Security Gateways (SEGs)

Security Gateways (SEGs) are entities on the borders of the IP security domains.

Each security domain can have one or more SEGs. Each SEG is defined to handle traffic in or out of the security domain towards a well-defined set of reachable IP security domains.

The number of SEGs in a security domain depends on the need to differentiate between the externally reachable destinations, the need to balance the traffic load and to avoid single point of failures. In practicality, the security gateways are defined by functionality and are expected to physically coincide with the border gateways already defined for the GTP core network architecture. More information on SEGs can be found in 5.2 and section 6.

SEGs are responsible for security sensitive operations and shall be physically secured.

4.6 Key Administration Centres (KACs)

4.6.1 KACs for native IP based protocols

Key Administration Centres (KACs) are entities that are used for negotiating inter-domain SAs on behalf of Security Gateways (SEGs).

The following are the most important tasks for a KAC:

- Perform SA negotiation with KACs belonging to other network operators.
- Distribute negotiated SA(s) to requesting nodes belonging to the same network as the KAC.
- Negotiate and establish IPsec protected communication with NEs or SEGs in its own network.

- Enforce security policies for the interworking between networks.

KACs are responsible for security sensitive operations and shall be physically secured.

4.6.2 KACs for SS7 and SS7/IP mixed protocols

Key Administration Centres (KACs) are entities that are used for negotiating MAPsec SAs on behalf of MAP-NEs.

When MAP-NEs need to establish a secure connection towards another MAP-NEs they 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 domains for which it is negotiated. That is, the same MAPsec SA shall be provided to all MAP-NE in security domain A when communication with MAP-NEs in security domain B. Each security domain can have one or more KACs. Each KAC will be defined to MAPsec SAs towards a well-defined set of reachable MAP security domains. The number of KACs in a security domain will depend on the need to differentiate between the externally reachable destinations, the need to balance the traffic load and to avoid single point of failures.

The following are the most important tasks for a KAC:

- Perform SA negotiation with KACs belonging to other network operators. This action is triggered either by request for an SA by a NE or by policy enforcement when MAP-SAs always should be available.
- Perform refresh of MAP-SAs. Triggered internally by MAP-SA lifetime supervision, which is depending on the policies set by the operator and if, it is decided during the negotiation.
- Distribute valid MAP-SAs to requesting nodes belonging to the same network as the KAC. This is done according to the MAP-SA transport procedures defined in section 7.2.4.
- Negotiate and establish IPsec protected communication with NEs in its own network

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

KACs are responsible for security sensitive operations and shall be physically secured.

5 Key management and distribution architecture for the UMTS core network

5.1 Security Associations (SAs)

In the UMTS network domain security architecture, the keys, used to provide message confidentiality and integrity, together with the algorithms as well as other security parameters form Security Associations. Therefore, the key management and distribution are handled by Internet Key Exchange (IKE) [19,20,21]. The main purpose of IKE is to negotiate, establish and maintain Security Associations between two parties to establish secure connections.

The concept of a Security Association is central to IPsec. A SA defines a one way secure connection. Typically, to secure a bi-directional communication between two parties, two Security Associations (one in each direction) are required.

An SA can be established for either AH or ESP, but not both. If both AH and ESP protection is required to protect a connection, then two (or more) SAs will be needed. Security associations are uniquely defined by the following parameters:

- A Security Parameter Index (SPI)
- An IP Destination Address
- A security protocol (AH or ESP) identifier

With regard to the use of security associations in the UMTS network domain control plane the destination address shall always be a unicast address.

The IPsec specification of SAs can be found in RFC-2401 [13].

NOTE: The above description assumes IPsec SAs. For MAPsec the SAs will be slightly different. Details of the MAPsec SAs are found in section 5.3, section 7 and Annex B.1.

5.1.1 Security Association functionality

IPsec offers a set of security services, which is determined by the negotiated security associations. That is, the SA defines which security protocol to be used, the mode and the endpoints of the SA.

In the UMTS NDS, the IPsec security protocol shall always be ESP. The SA mode shall be tunnel mode when one of endpoints is a security gateway. Otherwise, transport mode can be used. In NDS it is further mandated that integrity protection/message authentication together with anti-replay protection shall always be used.

The security service functionality that can be provided given the NDS requirements are:

- data integrity;
- data origin authentication;
- anti-replay protection;
- confidentiality (optional);
- limited protection against traffic flow analysis when confidentiality is applied.

5.1.2 Security Policy Database (SPD)

The Security Policy Database (SPD) is a policy instrument to decide which security services are to be offered and in what fashion.

The SPD shall be consulted during processing of both inbound and outbound traffic. This also includes traffic that shall not/need not be protected by IPsec. In order to achieve this the SPD must have unique entries for both inbound and outbound traffic such that the SPD can discriminate among traffic that shall be protected by IPsec that shall bypass IPsec.

The processing options are:

- **Discard**

  This option is used to explicitly disallow certain types of traffic to exit or enter the host or traverse the security gateway

- **Bypass IPsec**

  This option is used for traffic that is allowed to pass without IPsec protection

- **Apply IPsec**

  This option is used for traffic that shall be protected by IPsec. For such traffic the SPD must specify the security services to be provided, protocols to be employed, algorithms to be used, etc.

If IPsec processing is to be applied, the SPD entry will include information on the following:

- the SA or SA bundle to be used;
- the IPsec protocol(s) to be used;

- the mode(s);
- the algorithms to be employed;
- the nesting requirements, if there is any.

5.1.3 Security Association Database (SAD)

The Security Association Database (SAD) contains parameters that are associated with the active security associations. Every SA has an entry in the SAD. For outbound processing, a lookup in the SPD will point to an entry in the SAD. If an SPD entry does not point to an SA that is appropriate for the packet, an SA (or SA-bundle) shall be automatically created.

For inbound processing the following packet fields are used for looking up the SA in the SAD:

- Outer Header's Destination IP address (either the IPv4 or IPv6 destination address);
- IPsec Protocol;
- SPI (a32-bit value used to distinguish among different SAs terminating at the same destination and using the same IPsec protocol).

The following SAD fields are used during IPsec processing (AH specific fields omitted):

- Sequence Number Counter (a 32-bit value used to generate the Sequence Number field in the ESP header);
- Sequence Counter Overflow (a flag to indicate the appropriate action when sequence number overflows occur);
- Anti-Replay Window (an interval of counter numbers used to determine whether an inbound ESP packet is a replay);
- ESP Encryption algorithm, keys, mode, IV, etc;
- ESP authentication algorithm, keys, etc;
- Lifetime of this Security Association (the lifetime interval may be expressed as a time or byte count, or both, the first lifetime to expire taking precedence).
- IPsec mode;
- Path Maximum Transfer Unit (MTU).

5.1.4 SA bundles and SA combinations

An individual SA defines exactly one security protocol, either AH or ESP, but not both. Sometimes a security policy has requirements that cannot be handled by a single SA. In such cases it is necessary to employ more than one SA to satisfy the security policy. The term "SA bundle" is used for cases where more than one SA is required to satisfy a security policy. Note that the SAs that comprise a bundle may terminate at different endpoints. Security associations may be combined into bundles in two ways namely transport adjacency and iterated tunneling.

A basic set of combinations and configurations is defined in [13]. These include minimum functionality for passing security gateways and nesting of tunnels etc.

For the UMTS network domain control plane the requirements for nesting and combinations of SAs are covered in section 5.2 and section 6.

5.2 Use of the Internet Key Exchange protocol

The Internet Key Exchange (IKE) protocol shall be used for negotiation of both MAPsec SAs and IPsec SAs.

UMTS NDS shall support the use of pre-shared secrets for IKE SA authentication.

5.3 SA management and distribution architecture for native IP based protocols

5.3.1 Network domain security architecture outline

For native IP based protocols in UMTS network, SA negotiation and establishment are based on the IPsec IKE [13,19,20,21] protocol. Based on the security domain and interface concepts discussed in section 4.4.1, a given interface may be an intra-domain interface or an inter-domain interface. A security connection implies IPsec protected communications between two parties.

In each of the security domain, there exist one or more Key Administration Centre (KAC). In order to establish a secure connection over an inter-domain interface, SA is negotiated between two KACs on behalf of SEGs in each of its own security domain.

For an inter-domain security connection, Security Gateways (SEGs) shall engage in direct communication with entities in other security domains. The chained-tunnels can be used to provide hop-by-hop security. All traffic from a NE in security domain A toward a NE in security domain B will be first tunnelled to a SEG in its own security domain. Then an inter-domain tunnel will connect the two SEGs. Once the traffic reaches the SEG in the security domain B, it will be tunnelled to the destination NE. See Figure 1 for an illustration.

If the two parties belong to the same security domain and the communications do not pass through security gateways, then transport mode can be used to provide end-to-end security. The NEs and SEGs will be able to negotiate, establish, and maintain intra-domain SAs.

Between any two communicating entities only one ESP tunnel will be needed. This makes for coarse-grained security granularity.

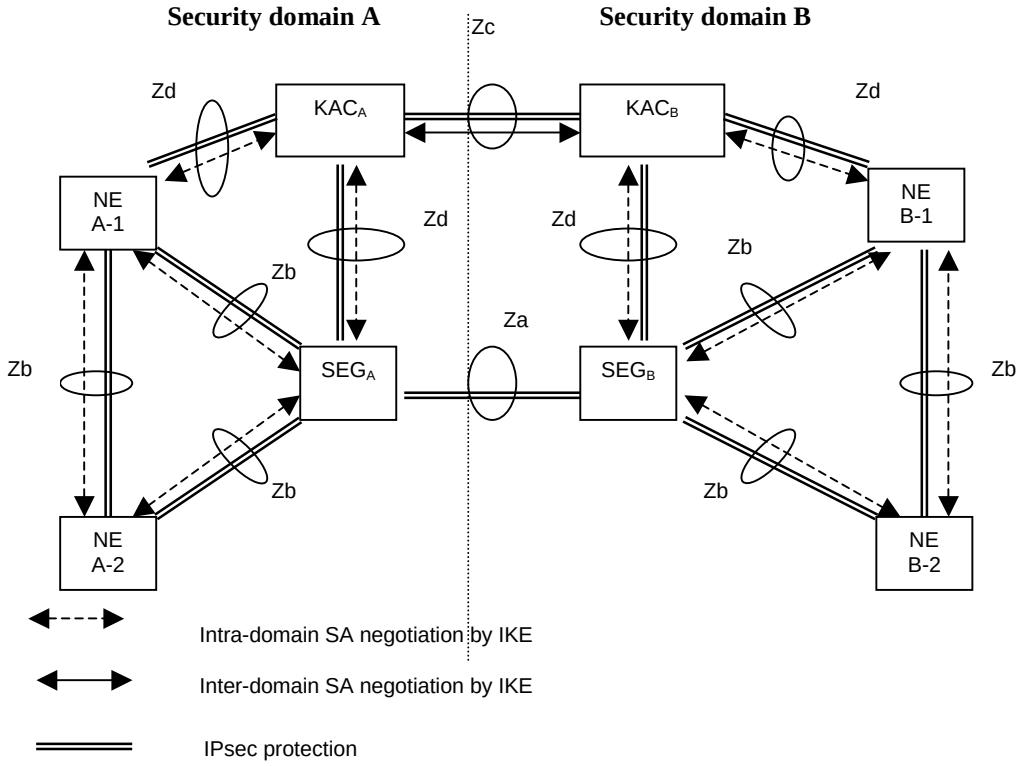

Figure 1: NDS architecture for IP-based protocols

5.3.2 Interface description

The following interfaces is defined for protection of native IP based protocols:

- **Za-interface (SEG-SEG)**

  The Za-interface covers all secure inter-domain IP communications. The Za interface is between two security gateways (SEGs)

  The security connection may use IPsec ESP in tunnel mode. The security associations for Za interface are negotiated by KACs on behalf of two parties. Normally ESP shall be used with both encryption and authentication/integrity, but an authentictaion/integrity only mode is allowed.

  When chained tunnels are used between two NEs, the tunnel between two SEGs can be used to deliver the traffic for different pairs of NEs. This will limit the number of SAs and tunnels that need to be maintained.

  SEGs shall not be used for the Gi interface.

- **Zb-interface (NE-SEG, NE -NE)**

  The Zb-interface is located between a NEs and a SEG or two NEs from the same security domain. The two parties are able to negotiate SAs, establish and maintain security protections between them. Whether the security protection is established when needed or a priori is for the security domain operator to decide. The security protection is subsequently used for exchange of secured traffic. Whether or not the application traffic actually terminates at the tunnel endpoints is irrelevant to the Zb-interface functionality.

  Normally ESP shall be used with both encryption and authentication/integrity, but an authentictaion/integrity only mode is allowed.

- **Zc –interface (KAC-KAC)**

  The Zc interface is between KACs from different security domains. The KACs negotiate inter-domain SAs on behalf of NEs or SEGs in each of its own domain over Zc interface. The ISAKMP phase 1 SA will be negotiated to protect the subsequential negotiation of SAs in client mode of IKE.

- **Zd – interface (KAC-NE, KAC –SEG)**

  Zd interface is between a KAC and a NE or a SEG. KAC and NE or SEG are able to negotiate intra-domain SAs, establish and maintain security protections between KAC and NE or SEG. Whether the security connection is established when needed or a priori is for the security domain operator to decide. The security connection is subsequently used for exchange of secured traffic between the KAC and the NE or SEG.

  Especially, negotiated inter-domain SAs over the Zc interface maybe distributed over Zd interface to SEGs.

NOTE-1: The security policy established over the Zc-interface is subject to roaming agreements. This differs from the security policy enforced over the Za, Zb, and Zd-interface, which is unilaterally decided by the security domain operator.

NOTE-2: There is no direct inter-domain SA negotiation for NEs or SEGs belonging to separate security domains. This is because it is important to have a clear separation between the security domains.

5.4 SA 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 the security mechanisms are found on the application layer a number of the issues are unique to the application. Section 7 contains detailed and specific requirements for the applicable application protocols.

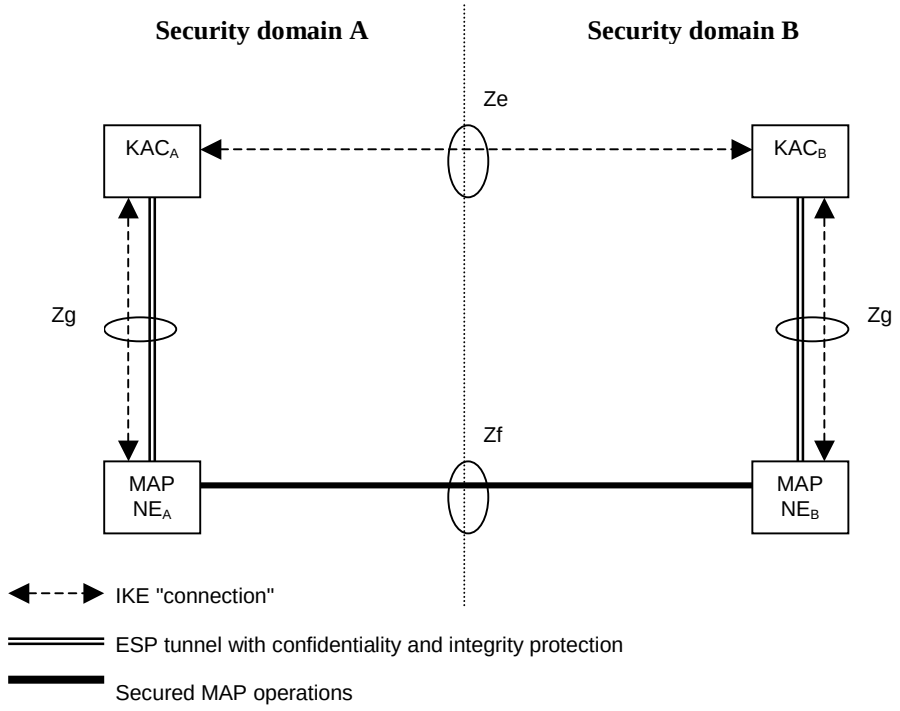

Figure 2: Overview of the Ze, Zf and Zg interfaces

For R4 the only SS7 protocol to be protected is the MAP protocol. References to MAP security (MAPsec) may therefore be extended to be more generic in later releases.

The following interfaces is defined MAPsec.

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

  The Ze-interface is used to negotiate MAPsec Security Associations (SAs) between MAP security domains. The traffic over Ze consists only of IKE negotiations. The negotiated MAPsec SAs are valid on a security domain to security domain basis. The KACs are expected to be additionally protected by firewalls etc towards the Ze-interface.

- **Zf-interface (KAC-NE)**

  The Zf-interface is located between MAP-NEs and a KAC from the same MAP security domain. The KAC and the MAP-NE are able to use IKE to negotiate, establish and maintain 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 transport of MAPsec SAs from the KAC to the MAP-NE. The HTTP protocol is used for transport of MAPsec SAs over the Zf-interface.

- **The Zg-interface (NE-NE)**

  The Zg-interface is located between MAP-NEs. The MAP-NEs may be from the same security domain or from 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 protected selectively as specified in the applied MAPsec security profile.

6 Security for native IP based protocols

6.1 Security services afforded to the protocols

The security services provided by using ESP in tunnel mode are:

- data integrity;
- data origin authentication;
- anti-replay protection;
- confidentiality (optional);
- limited protection against traffic flow analysis when confidentiality is applied;

6.2 Security for GTP

6.2.1 The need for protecting GTP-C

The GPRS Tunnelling Protocol (GTP) is defined in 3G TS 29.060 [5]. The GTP protocol includes both the GTP control plane signalling (GTP-C) and user plane data transfer (GTP-U) procedures. GTP is defined for Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs.

GTP-C is used for traffic that is sensitive in various ways including traffic that is:

- critical with respect to both the internal integrity and consistency of the network
- essential in order to provide the user with the required services
- crucial in order to protect the user data in the access network and that might compromise the security of the user data should it be revealed

Amongst the data that clearly can be considered sensitive are the mobility management messages, the authentication data and MM context data. Therefore, it is necessary to apply security protection to GTP signalling messages (GTP-C).

Network domain security does not cover protection of user plane data and hence GTP-U is not protected by NDS procedures.

6.2.2 Policy discrimination of GTP-C and GTP-U

GSNs must be able to discriminate between GTP-C messages, which shall receive protection, and other messages, including GTP-U, that shall not be protected. Since GTP-C is assigned a unique UDP port-number [5] IPsec can easily distinguish GTP-C datagrams from other datagrams that may not need IPsec protection.

As discussed in section 5.1.2 the Security Policy Database (SPD) is consulted for all traffic (both incoming and outgoing) and it processes the datagrams in the following ways:

- discard the datagram
- bypass the datagram (do not apply IPsec)
- apply IPsec

Under this regime GTP-U will simply bypass IPsec while GTP-C will be further processed by IPsec in order to provide the required level of protection. The SPD has a pointer to an entry in the Security Association Database (SAD) which details the actual protection to be applied to the datagram.

NOTE: Selective protection of GTP-C relies on the ability to uniquely distinguish GTP-C datagrams from GTP-U datagrams. For R99 on onwards this is achieved by having unique port number assignments to GTP-C and GTP-U. For previous version of GTP this is not the case.

6.2.3 Security policy granularity

The policy control granularity afforded by NDS is determined by the degree of control with respect to the ESP tunnels between the NEs. The normal mode of operation is that only one ESP tunnel is used between any two NEs and therefore the security policy will be identical to all secured traffic passing between the NEs.

This is consistent with the overall NDS concept of security domains, which should have the same security policy in force for all traffic within the security domain. Security policy enforcement for inter-domain communication is matter for the communication security domains and will be enforced by the SEGs of the communicating security domains.

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

[EDITOR: What exactly is the status of the MAPsec RFC ?. Has it got a number yet so that we can reference it? I guess the RFC cannot be produced until we have agreed on this TS.]

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 Ze 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.

The SPD may be implemented as a text file to ease the porting to different systems. Text-file based implementation is also easier to alter by possible third parties than a GUI interface. The SPD file contains the information required to implement the security policy and does not require a lot of memory. It can be easily cached to improve the performance of the system (real time requirements).

7.2.4 MAPsec SA transport protocol for the Ze-interface

The protocol to be used as transport protocol for the MAPsec SAs is HTTP. The use of HTTP implies that the KAC should then run a standard WEB server with a standard HTTP database to contain the MAPsec SAs.

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

NOTE: HTTP, through the use of TCP, has acknowledgement of the messages. The procedures therefore contains no explicit acknowledgement.

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.

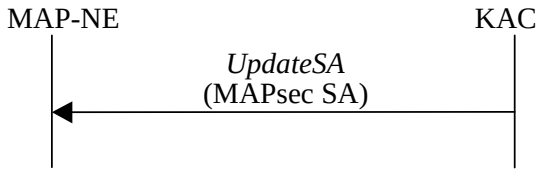

Figure 5: UpdateSA procedure

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.

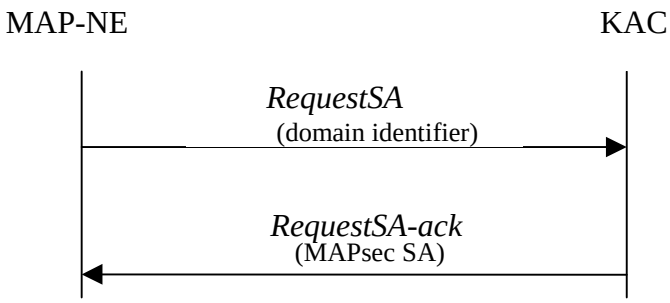

Figure 6: RequestSA procedure

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

8 Security for the Iu/Iur-interfaces

ffs

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

This annex gives an overview of the features of IPsec that is used by in the UMTS network domain. The overview given here defines a minimum set of features that must be supported. In particular, this minimum set of features is required for interworking purposes and constitutes a well-defined set of simplifications.

The accumulated effect of the simplifications is quite significant in terms of reduced complexity. This is achieved without sacrificing security in any way. It shall be noted explicitly that the simplifications are specified for the UMTS network domain control plane and that they may not necessarily be valid for other network constellations and usages.

Within their own network, operators are free to use IPsec features not described in this annex although there should be no security or functional reason to do so.

A.1 Usage of IPsec payload compression

Standard IPsec allows for packet payload compression to be used in conjunction with ESP and AH (RFC-2393, [12]). For the purpose of the UMTS network domain control plane, use of stateless packet-by-packet compression in general offers no benefits since the compression is not effective for small packets.

However, the disadvantages of introducing payload compression are added complexity for the SA negotiation phase since separate compression SAs must be negotiated and added complexity in the packet processing for both the sending and the receiving side.

Therefore IPsec payload compression shall not be used for interworking traffic over the Za-interface.

A.2 Support of ESP

IPsec provides two different security protocols. These are Authentication Header (AH) and Encapsulating Security Payload (ESP).

- The IP Authentication Header (AH) (RFC-2402, [14]) provides connectionless integrity, data origin authentication, and an optional anti-replay service.
- The Encapsulating Security Payload (ESP) protocol (RFC-2406, [18]) may provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service. (One or the other set of these security services must be applied whenever ESP is invoked.)
- The scope of the integrity protection afforded by AH is somewhat wider than that of ESP since AH includes partial coverage of the (outer) IP header. However, in practice this has limited security significance and for the purpose of the UMTS network domain control plane the security services difference is minimal. Since AH does not offer confidentiality services and since ESP essentially can cover all of AHs services, only ESP is mandated for the UMTS network domain control plane.

When IPsec is applied, the ESP security protocol shall be used for all interworking traffic. Furthermore, ESP shall always be used with integrity, data origin authentication, and anti-replay services. That is, the NULL authentication algorithm is explicitly not allowed for use in the UMTS network domain control plane.

A.3 Support of tunnel mode

IPsec provides two different modes of operation for the security protocols. The modes are:

- *transport mode;* In transport mode the protocols provide protection primarily for upper layer protocols.
- *tunnel mode;* In tunnel mode the protocols are applied to tunnelled IP packets. Only tunnel mode can pass through security gateways.

Since security gateways are an integral part of the UMTS network domain control plane architecture tunnel mode shall be supported. For interworking purposes, security gateways shall be used and consequently only tunnel mode is applicable for this case.

The operators may support transport mode within their own network, but it shall be noted that tunnel mode alone will be sufficient for all cases. There is therefore no explicit need for support of transport mode in the UMTS network domain control plane.

A.4 Support of ESP encryption transforms

IPsec offers a fairly wide set of confidentiality transforms. The only transform that compliant IPsec implementation is required to support is the ESP_DES transform. However, the Data Encryption Standard (DES) transform is no longer considered to sufficiently strong in terms of cryptographic strength. This is also noted by IESG in a note in RFC-2407 [19] to the effect that the ESP_DES transform is likely to be deprecated as a mandatory transform in the near future. A new Advanced Encryption Standard (AES) is being standardized to replace the aging DES.

It is therefore explicitly noted that for use in the UMTS network domain control plane the ESP_DES transform shall not be used.

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 endpoint: hop-by-hop shall always be used, if the packet has to pass through security gateways.
- Security protocol: ESP shall always be used.
- Mode: tunnel mode shall always be used when at least one of the endpoints is a security gateway.
- 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

[Editor: It seems unwise to proceed with the MAPsec profiles before we have a clear idea of what the MAPsec DoI RFC will contain.]

B.2 UMTS Security Profile for GTP

[Editor: Formally GTP protection is part of R5 so this part is not so urgent. Nevertheless, we'd still like to complete this section at SA#17. (this requires some input though)]

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