3GPP TS 33.xxx V0.0.1 (2001-04)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group SA3
3G Security;
Network Domain Security: IP Network Layer Security
(Release 5)

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

IP is introduced as the network layer in the GPRS backbone network and then later in the UMTS network domain. It 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. From a security point of view, a whole new set of threats and risks must be faced.

Control plane signalling is transported by IP protocols inside and between core networks. This means that security solutions must be found for IP based protocols.

The security services that have been identified as being needed are confidentiality, integrity, authentication and anti-replay protection.

1 Scope

The present document defines the security architecture for the UMTS network domain IP based control plane. The scope of the UMTS network domain control plane is to cover the control signalling in the UMTS core network.

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 cryptographical integrity mechanism in place.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

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

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

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

Transport mode: Mode of operation that primarily protects the payload of the IP packet, in effect giving protection to higher level layers

Tunnel mode: Mode of operation that protects the whole IP packet by tunnelling it so that the whole packet is protected

3.2 Symbols

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

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 two SEGs, a NE and a SEG, or two NEs belonging to different security domains in native IP network
Zb	Interface between a SEG and a NE or between two NEs within the same security domain in native IP network
Zc	Interface between two KACs belonging to different security domains in native IP networks
Zd	Interface between a KAC and a NE or a SEG within the same security domain in native IP network

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
IETF	Internet Engineering Task Force
IESG	Internet Engineering Steering Group
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security - a collection of protocols used for protection of IP protocols
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 the notion of a network security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks and hence separate security domains.

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.

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 their own security domains. After SAs have been negotiated, the KACs then 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.

For native IP-based protocols, security shall be provided at the network layer. The security protocols to be used at the network layer are the IPsec security protocols as specified in RFC-2401 [13]. All network domain entities supporting native IP-based control plane protocols shall support IPsec.

Secure communication between security domains may take place through Security Gateways (SEGs). In this case, a chained-tunnel/hub-and-spoke approach is used which facilitates hop-by-hop based security protection. This allows for lawful interception points and NATs in the networks.

If network configuration is allowed, for example, in IPv6 environment, the transport mode may be employed to provide end-to-end security without passing through SEGs. Furthermore, a chained tunnel approach may include only one SEG.

Although IPsec allows for manual entry of SAs, key management for IPsec between security domains shall always be automated in order to support IPsec anti-replay protection.

4.2 Security domains

4.2.1 Security domains and interfaces

The UMTS network domain shall be logically and physically divided into security domains. These control plane security domains, which may closely correspond to the core network of a single operator, 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 lists all the communication interfaces protected by Network Domain Security protocols.

Table 1: Network domain security specific interfaces

Interface	Description
Za	Between two SEGs, an NE and an SEG, or two NEs in different security domains. The inter-domain security associations used to protect the communications over this interface are negotiated over Zc interface by KACs.
Zb	Between an SEG and an NE or two NEs within the same security domain. The intra-domain security associations are negotiated over this interface to protect the communications over the same interface.
Zc	Between two KACs in different security domains. The inter-domain security associations are negotiated over this interface on the behalf of NEs or SEGs.
Zd	Between a KAC and an NE or an SEG in the same security domain. The intra-domain security associations may be negotiated over this interface. KAC may distribute inter-domain SAs to NEs or SEGs via this interface under the protection defined by the intra-domain security association.

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.

Table 2: Interfaces that are affected by network domain security

Interface	Description	Affected protocol	Security implication
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
Gs	Interface between SGSN and VLR/MSC	MAP	MAPsec shall be supported

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

4.2.2 Security termination points

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

IP security in the UMTS network domain control plane is based on a chained-tunnels. This implies that every end-point of a tunnel must be viewed as a termination point unless one uses nested tunnels. The only defined tunnel termination points are the communicating entities themselves and possibly one or more SEGs.

NOTE: Only network entities belonging to the security domains of the communicating entities can be security termination points. This holds irrespective of the fact that there may be intermediate networks between the communicating parties.

4.3 Security Gateways (SEGs)

Security Gateways (SEGs) are entities on the borders of the IP security domains and will be used for securing native IP based protocols. The SEGs are defined to handle communication over these interfaces:

- the Za-interface, which is located between SEGs from different IP security domains. The IPsec ESP in tunnel mode shall be used over this interface.

- the Zb-interface, which is located between an SEG and an NE within the same security domain. The intra-domain SAs are negotiated over this interface and the IPsec ESP in tunnel mode may be used over this interface.

All NDS related IP traffic may pass through a SEG before entering or leaving the security domain. Each security domain can have one or more SEGs. Each SEG will be 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 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.

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

4.4 Key Administration Centres (KACs)

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

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.

5 Key management and distribution architecture for the UMTS core network

5.1 Security Associations (SAs)

In the UMTS network domain security architecture the key management and distribution between SEGs and between KACs is handled by the IPsec protocol Internet Key Exchange (IKE) [19,20,21]. The main purpose of IKE is to negotiate, establish and maintain Security Associations between parties that are to establish secure connections. The concept of a Security Association is central to IPsec. The SAs defines uni-directional "connections" which serves to provide the security protocols ESP and AH with keys etc.

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. To secure typical, bi-directional communication between two hosts, or between two security gateways, two Security Associations (one in each direction) are required.

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 following is noted:

- The destination address shall always be a unicast address (in compliance with IPsec requirements)
- NDS only requires support for tunnel mode SAs. IPsec requirements for transport mode SAs does not apply for NDS.
- NDS only requires support for ESP SAs. IPsec requirements for AH SAs does not apply for NDS.

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

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 SA mode and the endpoints of the SA.

In the UMTS NDS the IPsec security protocol shall always be ESP and the SA mode shall always be tunnel mode. 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;
- any 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 or fetched from an SEG or KAC.

For inbound processing the following IP header 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; (for the UMTS network domain control plane this shall always be ESP)
- 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; (a 32-bit counter used to determine whether an inbound ESP packet is a replay)
- ESP Encryption algorithm, keys, IV mode, IV, etc; (for NDS the ESP_DES transform shall not be used)
- ESP authentication algorithm, keys, etc; (for NDS this field shall not be null)
- 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 protocol mode; (for NDS only tunnel mode shall be used)
- Path Maximum Transfer Unit (MTU)

NOTE: The SAD processing rules to and the SAD fields mentioned above does not apply to MAPsec.

5.1.4 SA bundles and SA combinations

The traffic over an individual SA is protected by 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 that 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 inter-domain and intra-domain IPsec SAs.

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

5.3 Key management and distribution architecture

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. Annex A gives an overview over the usage of IPsec in NDS.

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 or NEs in each of its own security domain.

For an inter-domain security connection, Security Gateways (SEGs) may engage in direct communication with entities in other security domains. The chained-tunnels can be used to provide hop-by-hop security. See Figure 1 for an illustration.

If 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 for each direction only one SA will be needed. This makes for coarse-grained security granularity.

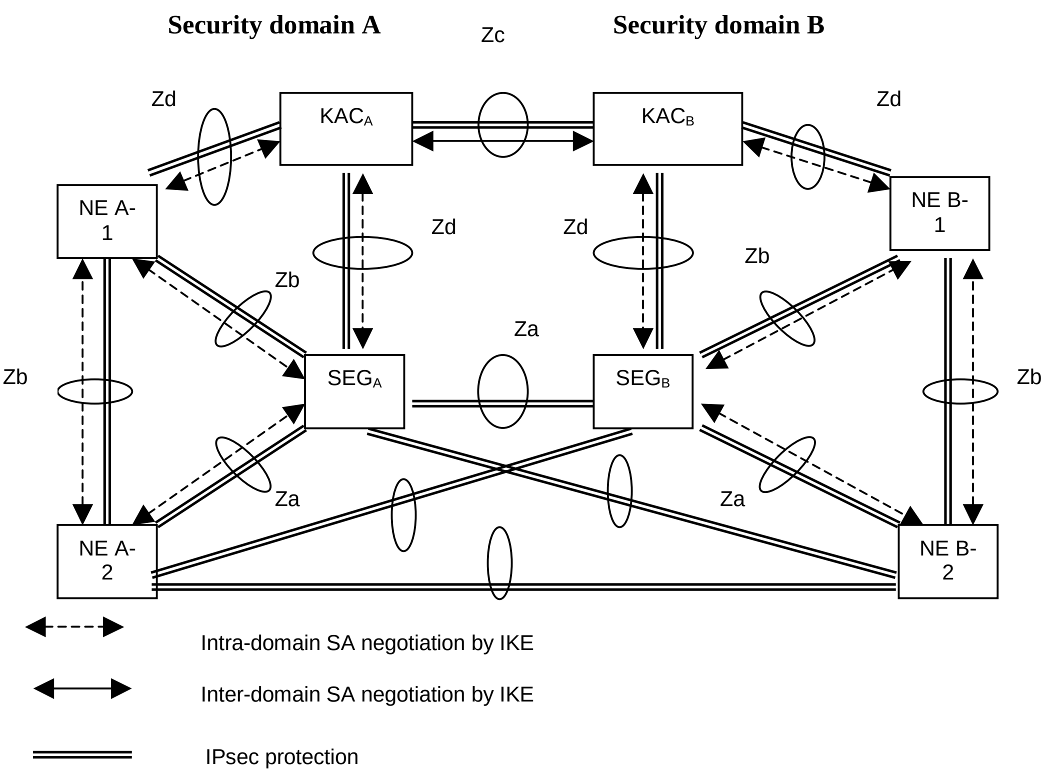

Figure 1: NDS architecture for IP-based protocols

5.3.2 Interface description

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

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

  The Za-interface covers all secure IP communication between security domains. Subject to roaming agreements, the inter-SEG tunnels would normally be available at all times, but they can also be established as needed. This tunnel is subsequently used for forwarding secured traffic between security domain A and security domain B.

  One SEG can be dedicated to only serve a certain subset of all roaming partners. This will limit the number of SAs and tunnels that need to be maintained. The number of SEGs within a network will normally be limited.

  Some inter-domain communications from domain A to domain B may be tunnelled from an SEG in domain A to an NE in domain B or from an NE in domain A to an SEG in domain B, if the network protocol is allowed.

  If the network protocol is allowed, the inter-domain communications from domain A to domain B may be protected from one NE to another NE by ESP either in transport mode or tunnel mode.

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

The Zb-interface is located between an NE and an SEG or between two NEs from the same security domain. If an SEG is used to forward inter-domain communications, the NE and the SEG should be able to establish and maintain ESP-tunnels between them. Whether the tunnel is established when needed or a priori is for the security domain operator to decide. The tunnel is subsequently used for exchange of secured traffic between the NE and the SEG.

Intra-domain communications between two NEs should be protected by either ESP tunnel mode or ESP transport mode.

Normally ESP shall be used with both encryption and authentication/integrity, but an authentication/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 an NE or an SEG. KAC and NE (or SEG) should be 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.

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

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

6.2.2 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 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

SGNs 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 or SEGs. The normal mode of operation is that only one ESP tunnel is used between any two NEs or SEGs, 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 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

When IPsec is applied, the ESP (RFC-2406, [18]) 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

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 (RFC-2401, [13]) 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 and instead the ESP_AES transform shall 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.

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 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): Network Address Translators (NATs), filtering routers and firewalls

C.1 Network Address Translators (NATs)

Network Address Translators (NATs) are not designed to be part of the UMTS network domain control plane. Since network domain security employs a chained-tunnel approach it may be possible to use NATs provided that the network is carefully configured.

C.2 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.

Annex D (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**