3GPP TSG SA WG3 Security — S3#18 **S3-010148**

21 - 24 May, 2001

Phoenix, Arizona, USA

From: Telenor (NDS Rapporteur)

Title: Update information on TS33xxx v050 (from TS33200 v035)

Update information on TS33xxx

This document gives a brief summary of the process of creating TS33xxx v050 from the basis of TS33200 v035. (TS33200 v035 (**S3z010004**) was the last version of TS33200 that contained both NDS/SS7 and NDS/IP related material.)

It should be noted that Motorola have already provided a similar draft input (**S3z010022**), but since Motorola's draft TS changes some of SA3 already agreed working assumptions I have had to produce a version that complies with our current working assumptions[1].

I've attempted to make TS33200 v050 and TS33xxx v050 look as similar in style as the contents allow for.

Section	**Changes**
Title page	New Title and Release …
Introduction	Minor modifications to reflect that this TS is NDS/IP
1. Scope	Copied from S3z010022. Reference to LI specification removed.
2. References	Removed: 29.002, 33.106 / 33.107, 33.800 Added: 33.200 NDS/MAPsec
3.1 Definitions	SA – Added some bits from S3z010022 on SAs
3.2 Symbols	Redundant MAPsec related symbols removed • C, D, E, F • Gc, Gd, Gf, Gr, Gs • Iu, Iur Zd, Ze, Zf and interfaces marked as MAPsec interfaces and retained.
3.3 Abbreviations	MAPsec related abbreviations removed, but MAPsec itself retained. RNS, USP and TVP also removed. NDS/IP and NDS/MAP added.
4	Title changed to " Overview over UMTS network domain security IP based protocols "
4.1 Introduction	Split into "Introduction" and "Protection at the network layer" in much the same manner as for TS33200 v050.
4.2 Protection…	Old 4.2 deleted. New 4.2: "Protection at the network layer"
4.3 Security …	Some material is moved between 4.2 and 4.3
4.4.1 Security …	Minor modifications to the main text and table-1. MAPsec material removed from Table-2.
4.4.2 Security…	Removed
4.6 KACs	Removed
5.1	New section 5.1 included to list the security services. Old 5.1 now becomes 5.2: Removal of some MAPsec material in addition to removal of some tutorial material
5.3 Profiling of IPsec in NDS/IP	New. Since the number of sections in the main body of the document has decreased and since the structure of the document is more focused I found that it probably would improve the structure if the material in Annex A was to section 5. So 5.2 now contains the material from Annex A.
5.4 Use of IKE	Renamed "Profiling of IKE in NDS/IP".

[1] SA3#18 may want to endorse Motorola's draft TS as the starting point instead of this draft TS.

	Some profiling information added in accordance with the presentation (S3z010012) given at S3#17bis. The presentation was well received and I interpreted the meeting to generally agree to the contents in S3z010012.
5.4 Key mngt for SS7 …	Removed
5.5 Key mngt for NDS/IP	Largely kept as-is. 5.5.2: NOTE-2: Tried to clarify the Zc (NE←→NE) interface can be between security domains, provided that the possibly different security policies are enforced by the NE (which then logically will contain SEG functionality).
6	Renamed to "Security protection for GTP"
7. Security for SS7…	Removed
Annex B	To follow the style from TS33200 I have moved the protection profile into a section in the main body of the document. So the old annex B is removed. Experimentally, I have included a new informative annex B to sketch out a possible evolution of NDS to allow for a PKI type of authentication framework for NEs. The same material is also submitted as a separate contribution. *The material in this annex is independent of the contents in the rest of the draft TS. The annex can therefore easily be removed.*
Annex C NATs and FW	Now Annex A. I had originally decided to propose to remove this annex due to a lack of contributions and interest, but since Nokia had prepared a contribution on this topic for the S3#17bis I have changed my mind. Hopefully Nokia will resubmit their contribution…

/Geir M. Køien, Telenor R&D

3GPP TS 33.xxx V0.5.0 (2001-05)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group SA3
3G Security;
Network Domain Security;
IP network layer security
(Release 5)

Keywords

Security, IPsec, 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 the core network. This was formerly perceived not to be a problem, since the 2G networks previously were the provinces of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions. 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.

This technical specification is the stage-2 specification for IP related security in the UMTS core network.

The security services that have been identified as being needed are confidentiality, integrity, authentication and anti-replay protection. These will be ensured by standard procedures, based on cryptographic techniques.

1 Scope

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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

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

[2] 3G TS 21.905: 3G Vocabulary

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

[4] 3G TS 29.060: GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface

[5] 3G TS 33.102: Security Architecture

[6] 3G TS 33.103: Security Integration Guidelines

[7] 3G TS 33.120: Security Objectives and Principles

[8] 3G TS 33.200: Network Domain Security; MAP application layer security

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

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

[11] RFC-2402: IP Authentication Header

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

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

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

[15] RFC-2406: IP Encapsulating Security Payload

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

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

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

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

[20] RFC-2411: IP Security Document Roadmap

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

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

[23] 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 unidirectional logical connection created for security purposes. All traffic traversing an IPsec SA is provided the same security protection. The IPsec SA itself is set of parameters to define a unidirectional security protection between two entities. An IPsec 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:

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
Za	Interface between SEGs belonging to different networks/security domains
Zb	Interface between SEGs and NEs within the same network/security domain
Zc	Interface between NEs within the same network/security domain
Zd	MAPsec interface between KACs belonging to different networks/security domains
Ze	MAPsec interface between KACs and MAP-NEs within the same network
Zf	MAPsec interface between networks/security domains for secure interoperation.

3.3 Abbreviations

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

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

GTP	GPRS Tunnelling Protocols
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP security - a collection of protocols and algorithms for IP security incl. key mngt.
ISAKMP	Internet Security Association Key Management Protocols
IV	Initialisation Vector
MAC	Message Authentication Code
MAPsec	MAP security
NAT	Network Address Translator
NDS	Network Domain Security
NDS/IP	NDS for IP based protocols
NDS/MAP	NDS for MAP/MAPsec
NE	Network Entity
PS	Packet Switched
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

4 Overview over UMTS network domain security for IP based protocols

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.

4.2 Protection at the network layer

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 IETF defined IPsec security protocols as specified in RFC-2401 [10]. All network domain entities supporting native IP-based control plane protocols shall support IPsec.

4.3 Security for native IP based protocols

The UMTS network domain control plane is 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.

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 not encompass the user plane Gi-interface towards other, possibly external to UMTS, IP networks.

A chained-tunnel/hub-and-spoke approach is used which facilitates hop-by-hop based security protection.

All secure communication between security domains shall take place through Security Gateways (SEGs). 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.

4.4 Security domains

4.4.1 Security domains and interfaces

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

The specific network domain security interfaces is found in table 1. The definitions for Zd, Ze and Zf only apply to NDS/MAP (TS33.200, [8]).

Table 1: Network domain security specific interfaces

Interface	Description	Network type
Za	Network domain security interface between SEGs. The interface is used for both the negotiation of security associations and for the set-up of ESP protected tunnels between SEGs (no third party negotiation).	IP
Zb	Network domain security interface between SEGs and NEs within the same network. The interface is used for both the negotiation of security associations and for the set-up of an ESP protected tunnel.	IP
Zc	Network domain security interface between NEs within the same network. The interface is used for both the negotiation of security associations and for the set-up of an ESP protected tunnel.	IP
Zd	MAPsec inter-domain interface. The Zd-interface is defined for negotiation of MAP security associations between KACs.	IP
Ze	MAPsec interface between KAC and MAP-NE within the same network. The interface is security protected by means of an IPsec ESP tunnel.	IP
Zf	MAPsec interface between MAP-NEs engaged in security protected signalling (applies to MAP-NEs belonging to different or even to the same security domain)	SS7/MAP

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

Table 2: Interfaces that are affected by NDS/IP

Interface	Description	Affected protocol	Security implication
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.

NOTE: NDS/IP is application layer protocol independent and other protocols than GTP may be supported in later version of this specification.

4.5 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 IKE and ESP protocols shall be used over this interface.

- the Zb-interface, which is located between a SEG and an NE within the same security domain. The IKE and ESP protocols may be used over this interface.

All NDS/IP traffic shall 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 all 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. The security gateways shall be responsible for enforcing security policies for the interworking between networks. The security may include filtering policies and firewall functionality not required in this specification.

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

5 Key management and distribution architecture for NDS/IP

5.1 Security services afforded to the protocols

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 services provided by NDS/IP:

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

5.2 Security Associations (SAs)

In the UMTS network domain security architecture the key management and distribution between SEGs is handled by the IPsec protocol Internet Key Exchange (IKE) [16,17,18]. 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.

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 identifier

With regard to the use of security associations in the UMTS network domain control plane the following is noted:

- NDS/IP only requires support for tunnel mode SAs
- NDS/IP only requires support for ESP SAs.

The IPsec specification of SAs can be found in RFC-2401 [10].

5.2.2 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 and that shall bypass IPsec.

The SPD plays a central role when defining security policies, both within the internal security domain and towards external security-domains. The security policy towards external security domains will be subject to roaming agreements and shall be regulated by a well-defined set of standardised NDS/IP protection profiles.

5.2.3 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.

5.2.4 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 handles 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 were 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 [10]. These include minimum functionality for passing security gateways and nesting of tunnels etc.

5.3 Profiling of IPsec in NDS/IP

This section gives an overview of the features of IPsec that is used by NDS/IP. 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 NDS/IP 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 section although there should be no security or functional reason to do so.

5.3.1 Support of IPsec payload compression

Standard IPsec allows for packet payload compression to be used in conjunction with ESP and AH (RFC-2393, [9]). For the purpose of NDS/IP, use of stateless packet-by-packet compression in general offers no benefits since the compression is not effective for the comparatively small packets that are protected by NDS/IP.

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.

5.3.2 Support of ESP

When NDS/IP is applied, only the ESP (RFC-2406, [15]) security protocol shall be used for all NDS/IP inter-domain control plane 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 NDS/IP.

5.3.3 Support of tunnel mode

Since security gateways are an integral part of the NDS/IP architecture, tunnel mode shall be supported. For NDS/IP inter-domain communication, security gateways shall be used and consequently only tunnel mode (RFC-2401, [10]) 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 NDS/IP.

5.3.4 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 [16] 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 NDS/IP, the ESP_DES transform shall not be used and instead the ESP_AES transform shall be mandatory.

5.4 Profiling of IKE in NDS/IP

The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following additional requirement on IKE is made mandatory for inter-domain SA negotiations over the Za-interface.

For IKE phase-1:

- The use of pre-shared secrets for authentication shall be supported
- Only Main Mode shall be used
- Only Fully Qualified Domain Names (FQDN) shall be used
- Support of AES shall be mandatory for confidentiality
- Support of SHA-1shall be mandatory for integrity/message authentication

For IKE phase-2:

- Perfect Forward Secrecy is optional
- Only IP addresses or subnet identity types shall be mandatory address types
- Support of Notifications shall be mandatory

NOTE: When AES MAC is defined for IKE by the IETF it will also be made mandatory for IKE phase-1 in NDS/IP.

5.5 Security policy granularity

The policy control granularity afforded by NDS/IP 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/IP concept of security domains, which should have the same security policy in force for all traffic within the security domain. The actual inter-domain policy is determined by roaming agreements according to a standardised set of NDS/IP protection profiles. Security policy enforcement for inter-domain communication is a matter for the SEGs of the communicating security domains.

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

5.6.1 Network domain security architecture outline

The NDS/IP key management and distribution architecture is based on the IPsec IKE [10,16,17,18] protocol. As described in the previous section a number of options available in the full IETF IPsec protocol suite have been considered to be unnecessary for NDS/IP. Furthermore, some features that are optional in IETF IPsec have been mandated for NDS/IP and lastly a few required features in IETF IPsec have been deprecated for use within NDS/IP scope. Section 5.3 and 5.4 gives an overview over the profiling of IPsec and IKE in NDS/IP.

The compound effect of the design choices in how IPsec is utilized within the NDS/IP scope is that the NDS/IP key management and distribution architecture is quite simple and straightforward.

The basic idea to the NDS/IP architecture is to provide hop-by-hop security. This is in accordance with the *chained-tunnels* or *hub-and-spoke* models of operation. The use of hop-by-hop security also makes it easy to operate separate security policies internally and towards other external security domains.

In NDS/IP only the Security Gateways (SEGs) shall engage in direct communication with entities in other security domains. The SEGs will then establish and maintain IPsec secured ESP tunnels between security domains. These SEG-SEG tunnels will normally be established and maintained to be in permanent existence. The SEG will maintain logically separate SAD and SPD databases for each interface.

The NEs will be able to establish and maintain ESP secured tunnels as needed towards a SEG or other NEs within the same security domain. All traffic from a NE in one security domain towards a NE in a different security domain will be routed via a SEG and will afforded hop-by-hop security protection towards the final destination.

Operators may decide to establish only one ESP tunnel. This would make for coarse-grained security granularity. The benefits to this is that it gives a certain amount of protection against traffic flow analysis while the drawback is that one will not be able to differentiate the security protection given between the communicating entities. It shall still be possible to negotiate different SAs for different protocols.

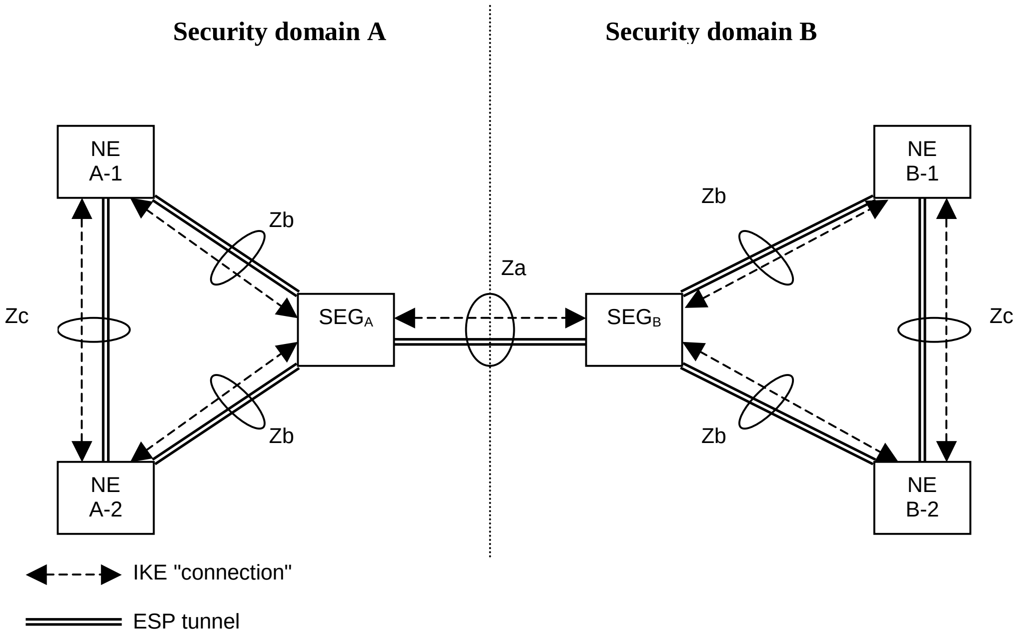

Figure 1: NDS architecture for IP-based protocols

5.6.2 Interface description

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

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

  The Za-interface covers all secure IP communication between security domains. The SEGs uses IKE to negotiate, establish and maintain a secure tunnel between them. Subject to roaming agreements, the inter-SEG tunnels would normally be available at all times, but they can also be established as needed. The 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 and should normally not be larger than the numer og BGs in the network.

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

  The Zb-interface is located between NEs and a SEG from the same security domain. The NE and the SEG are 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.

  Normally ESP shall be used with both encryption and authentication/integrity, but an authentication/integrity only mode is allowed. All control plane traffic towards external destinations shall be routed via a SEG.

- **Zc-interface (NE-NE)**

  The Zc-interface is located between NEs from the same security domain. The NEs are 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 NEs.

  Normally ESP shall be used with both encryption and authentication/integrity, but an authentictaion/integrity only mode is allowed. The ESP tunnel shall be used for all control plane traffic that needs security protection.

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

NOTE-2: There is normally no NE-NE interface for NEs belonging to separate security domains. This is because it is important to have a clear separation between the security domains. This is particularly relevant when different security policies are employed whithin the security domain and towards external destinations.

The restriction not to allow secure inter-domain NE-NE communication does not preclude a single physical entity to contain both NE and SEG functionality. A combined NE/SEG entity need not support an external Zb-interface provided that the entity itself is physically secured. The exact SEG functionality required to allow for secure inter-domain NE←→NE communication will be subject to the actual security policies being employed. Thus, it will be possible for roaming partners to have secure direct NE←→NE communication within the framwork of NDS/IP.

6 Security protection for GTP

This section details how NDS/IP shall be used when GTP is to be security protected.

6.1 The need for security protection

The GPRS Tunnelling Protocol (GTP) is defined in 3G TS 29.060 [4]. 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 is not intended to cover protection of user plane data and hence GTP-U is not normally protected by NDS/IP mechanisms.

6.2 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 in (TS29.060, [4]) IPsec can easily distinguish GTP-C datagrams from other datagrams that may not need IPsec protection.

As discussed in section 5.2.2 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 and 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 and provision of selective protection for GTP-C for pre-R99 versions of GTP is not possible.

6.3 Protection Profiles for GTP-C

Protection profiles for NDS/IP must be built up around the security policy concepts as managed by the SPD and the actual SAs as found in the SAD.

For practical purposes, this will allow a security domain operator to define a home domain policy and a separate policy towards all external destination domains.

In order to facilitate reliable and secure inter-domain communication a set of well-defined protection profiles is defined. Support for these profiles are mandatory for NDS/IP communication over the Za-interface. There are no mandatory protection profiles for intra-domain NDS/IP communication, but the inter-domain profiles can of course be employed internally if the operator so chooses.

6.3.1 Protection Profile 1

[EDITOR: OK, the following material isn't mature at all and isn't intended to be kept, but hopefully it will trigger contributions on the subject of NDS/IP protection profiles for GTP-C.]

This protection profile applies to GTP-C and shall identify GTP-C by means of the unique GTP-C portnumber as defined in TS29.060 ([4]).

This protection profiles defines the following:

- Integrity protection/message authentication **shall** be used.

  The selected algorithm is AES CBC MAC and the key length is 128-bits

- Confidentiality protection **shall** be used.

  The selected algorithm is AES and key length is 128-bits.

- Anti-replay protection **shall** be used

- SA lifetime shall be IPsec SA default lifetime (8 hours)

-

6.3.2 Protection Profile 2

6.3.3 Protection Profile 3

6.3.4 Protection Profile 4

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

A.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.

A.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 B (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**