From: Koien Geir [geir-myrdahl.koien@TELENOR.COM]
Sent: 04 December 2001 19:41
To: 3GPP_TSG_SA_WG3@LIST.ETSI.FR
Subject: SA3: Email approval of "for information" version of TS33210 NDS/I P

Hello SA3,

Here is the latest draft version of TS33210 NDS/IP together with an update-information description document.
All text in the document which are change marked or directly affected by the change marked text is open for discussion.
Explictly, the whole of Annex B and Annex C was left open for discussion by SA3#21.

The rest of TS33210 was agreed at SA3#21 and is therefore not open to general discussion, but still I'll be happy to be informed about typos and other obvious errors.

All issues with the current text and statements of objection or acceptance must be sent to the email exploder to be taken into account.

In lack of a defined procedure, I suggest the following procedure for this email approval:

1) 05.12.2001: Submit TS33210v080 for email approval. (this email, one day before the deadline)

2) 12.12.2001 1600 CET: Close-1: No more comments accepted.
If necessary, a new version will be distributed to the email list.
This is then a final opportunity to object to sending the draft TS33210 "for information" the SA plenary.
This version of the TS will be exactly the same as the one to be submitted to the SA plenary.

3) 13.12.2001 1600 CET: Close-2. Conclusions drawn.

(Maurice: For reference purposes, could you assign a Tdoc (SA3#22) and put the ZIP file on the server)

/Geir

Geir M. Køien
Telenor R&D
Servicebox 505
N-4898 GRIMSTAD, Norway

Gsm: +47 9075 2914

<<33210-080.zip>>

Update information

This document describes updates from version 070 to version 080.

The changes between v070 and v080 are mostly minor ones. There are a few editorial fixes like correcting reference numbers and table number etc. Then there are a few instances of now-redundant text that has also been deleted.

Change tracking note:

- Header info (version no. and month) exempted from change tracking
- TOC changes exempted form change tracking

To avoid excessive change bars (which would mask out the current marking) the following was exempted from change tracking:

- Moving “Security protection for GTP” from section 6 to Annex B
- Moving “Security protection of IMS protocols” from section 7 to Annex C

Open issues from SA3#21

Section 6 (Security protection for GTP) and section 7 (Security protection of IMS protocols) was not agreed at SA3#21. Thus, change bars have been kept as they were, except from a minor change done on-line at SA3#21 (which affects NOTE-2 on GTP-U in what is now Annex B.2).

As agreed section 6 and 7 has been moved to annex B and C respectively.
The whole of annex B and C is to be regarded as open with respect to the email approval.

Open issues to be handled later

As mentioned in S3-010670 we may consider specifying which IP version to use on the Za-interface in order to make sure that there are as few obstacles as possible to interoperability between security domains. Still, this part can safely wait until the ad-hoc in January or the SA3 plenary in late February.

- **Za-interface (SEG-SEG) (this issue has not yet been discussed by SA3)**
  Interoperability has been one of our main concerns for this interface. Given that the core network allows for both IPv4 and IPv6 to be used, we should realize that we have the potential problem of IP version incompatibility over Za.

  This potential problem could be addressed in various ways, including the following:
  - Requiring both IPv4 and IPv6 to be supported by all SEGs (dual stacks)
  - Requiring Transition Gateway (TrGW) services to be available to the SEGs in order to convert IKE-over-IPv4 to IKE-over-IPv6 and the other way around.
  - Requiring all SEGs to support one and only one IP version (preferably IPv6)
  - Allowing to types of SEGs:
    - SEG(IPv4) : Communicates only with other SEG(IPv4)
    - SEG(IPv6): Communicates only with other SEG(IPv6)

  Given that interoperability is a great concern to us, we should probably make a decision on this matter and specify exactly how communication over the Za-interface shall handled with respect to the IP version problem.

Update information –TS 33.210

The following table details the changes:

Section	Description
-all-	Except from clause 6.2 (=Annex B.2) and 7 (=Annex C), all marked changes in 33.210 v070 was "accepted".
Front page	Version & month changed. (no change bars)
TOC	The TOC was updated (without "track changes" on)
3.3. Abbreviations	Inclusion of TrGW. See also corresponding change to Annex A
GTP	Moved from section 6 to Annex B
IMS	Moved from section 7 to Annex C
Annex B	The previous Annex B has now become Annex D
5.2.1 SPD	Deletion of "*and shall be regulated by a well-defined set of standardised NDS/IP protection profiles*" from the last sentence. This part should have been removed quite some time ago when we decided that we were not going to standardize protection profiles for NDS/IP. (See also similar change to 5.5)
5.3.2 Support …	Changed Zc to Zb in the last sentence
5.3.4 Support of ESP authentication transforms	There were some formatting errors in the text that I corrected. So the resulting text is slightly different from the original proposed in contribution S3-010616 (Nokia).
5.4	Inclusion of "IKE SA lifetime" text. This was suggested in S3-01582 and agreed in principle by SA3#21, but the actual text was not presented to SA3#21 and thus this inclusion is open for discussion in the email appoval procedure.
5.5 Security Policy Granularity	Deletion of "*according to a standardised set of NDS/IP protection profiles*" from the second last sentence. This part should have been removed quite some time ago when we decided that we were not going to standardize protection profiles for NDS/IP. (See also similar change to 5.2.1)
5.6.1 NDS architecture outline	The last paragraph seemed to need a little clarification. So reformulated some of the text and hopefully made it more accurate. Figure-1: Changed Zc to Zb (no change bars here)
5.6.2	Definition of Za –interface Included an editor's note to say that we may consider specifying which IP version to use over Za in order to facilitate interoperability.
6.2 Interface description	For some reason the definition of Za now no longer says anything about the use of ESP. So I copied and adapted this from Zb into the Za-interface bullet point. Then additionally, I made a change to use the new "NDS/IP traffic" definition.
Annex A	Inclusion of TrGW. As mentioned in the update-information between v060 and v070 (S3-010670) we should probably mention TrGWs. So I have added some material on TrGW to annex A.There is also a corresponding update to the section 3.3 Abbreviations.
Annex B.2 (after the move)	NOTE-2: Changed the last sentence from: "*It should be noted that NDS/IP support for GTP-U is not mandatory.*" to "*It should be noted that NDS/IP support for GTP-U is outside the scope of this specification.*"

/Geir M. Køien, Telenor R&D

3GPP TS 33.210 V0.8.0 (2001-12)

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 security is to cover the control signalling on selected interfaces between UMTS network elements.

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 23.002: Network Architecture

[4] 3G TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2

[5] 3G TS 23.228: IP Multimedia (IM) Subsystem - Stage 2

[6] 3G TS 29.060: GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface

[7] 3G TS 33.102: Security Architecture

[8] 3G TS 33.103: Security Integration Guidelines

[9] 3G TS 33.120: Security Objectives and Principles

[10] 3G TS 33.203: Access security for IP-based services

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

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

[13] RFC-2402: IP Authentication Header

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

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

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

[17] RFC-2406: IP Encapsulating Security Payload

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

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

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

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

[22] RFC-2411: IP Security Document Roadmap

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

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

[25] 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.

NDS/IP Traffic: Traffic that requires protection according to the mechanisms defined in this specification.

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
Mm	Interface between a CSCF and an IP multimedia network
Mw	Interface between a CSCF and another CSCF
Za	Interface between SEGs belonging to different networks/security domains
Zb	Interface between SEGs and NEs and interface between NEs within the same network/security domain

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
CSCF	Call State Control Function
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
SIP	Session Initiation Protocol
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
TrGW	Transition Gateway

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.

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 [12].

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 NDS/IP traffic shall pass through a SEG before entering or leaving the security domain.

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.

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 the Za-interface, which is located between SEGs from different IP security domains. The IKE and ESP protocols shall 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 protocol Internet Key Exchange (IKE) [18,19,20]. 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 and IKE.

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 (this is the address of the ESP SA endpoint)
- A security protocol identifier (this will always be the ESP protocol in NDS/IP)

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
- There is no need to be able to negotiate SA bundles as only a single ESP SA is set up to protect traffic between the nodes

The IPsec specification of SAs can be found in RFC-2401 [12].

5.2.1 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 or that shall be discarded by 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~~.

5.2.2 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 shall be automatically created.

5.3 Profiling of IPsec in NDS/IP

This section gives an overview of the features of IPsec that are 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 ESP

When NDS/IP is applied, only the ESP (RFC-2406, [17]) security protocol shall be used for all NDS/IP inter-domain control plane traffic.

5.3.2 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, [12]) is applicable for this case.

The operators may support transport mode to protect communications between NEs within their own network (ie for the Zb ~~c~~ interface).

5.3.3 Support of ESP encryption transforms

IPsec offers a fairly wide set of confidentiality transforms. The transforms that compliant IPsec implementations are required to support are the ESP_NULL and the ESP_DES transforms. However, the Data Encryption Standard (DES) transform is no longer considered to be sufficiently strong in terms of cryptographic strength. This is also noted by IESG in a note in RFC-2407 [18] 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 it shall be mandatory to support the ESP_AES transform.

Editor's Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.

5.3.4 Support of ESP authentication transforms

The transforms that compliant IPsec implementation is required to support are the ESP_NULL, the ESP_HMAC_MD5 and the ESP_HMAC_SHA-1 transforms. For NDS/IP traffic ~~The~~ ESP shall always be used to provide integrity, data origin authentication, and anti-replay services ~~in NDS/IP~~, thus the ESP_NULL authentication algorithm is explicitly not allowed for use. ESP shall support ESP_HMAC_SHA-1 and AES MAC algorithms in NDS/IP.

Editor's Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.

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 in CBC mode shall be mandatory for confidentiality
- Support of SHA-1 shall be mandatory for integrity/message authentication

Phase-1 IKE SAs shall be persistent with respect to the IPsec SAs is derived from it. That is, IKE SAs shall have a liftetime for at least the same duration as does the derived IPsec SAs.

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.

Editor's Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.

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 [12,18,19,20] 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 for NDS/IP traffic. The SEGs will then establish and maintain IPsec secured ESP tunnels between security domains. SEGs will normally maintain at least one IPsec tunnel available at all times to a particular peer SEG. The SEG will maintain logically separate SAD and SPD databases for each interface.

The NEs may be able to establish and maintain ESP secured tunnels as needed towards a SEG or other NEs within the same security domain. All NDS/IP 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 between two communicating security domains. 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~~This does not preclude negotiation of finer grained security granularity at the discretion of the communicating entities.

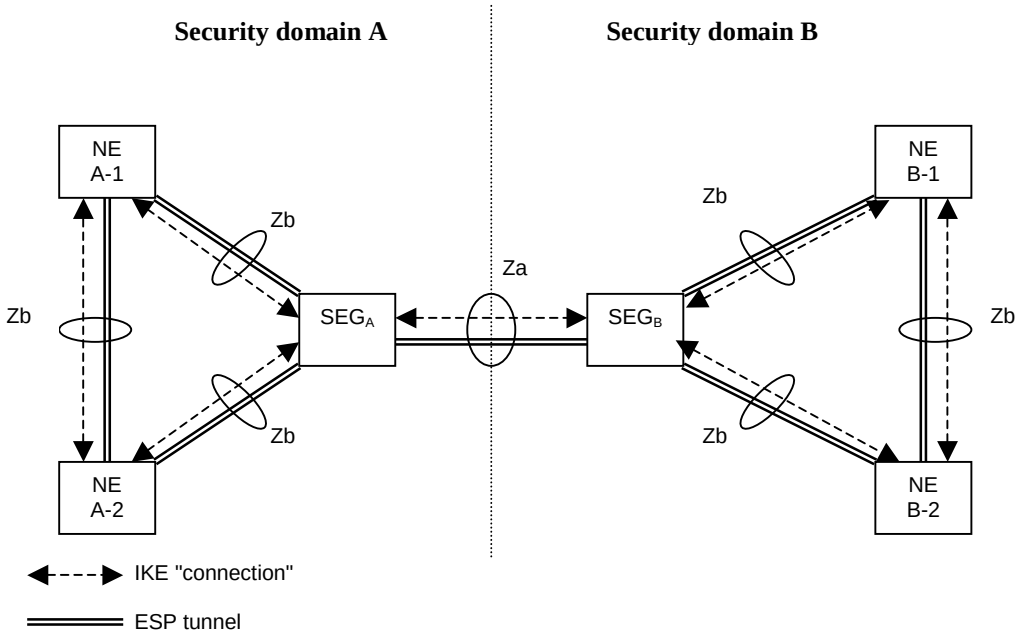

Figure 1: NDS architecture for IP-based protocols

5.6.2 Interface description

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

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

  The Za-interface covers all NDS/IP traffic between security domains. The SEGs uses IKE to negotiate, establish and maintain a secure ESP 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. ESP shall be used with both encryption and authentication/integrity, but an authentictaion/integrity only mode is allowed. The tunnel is subsequently used for forwarding ~~secured~~ NDS/IP 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.

  All security domains compliant with this specification ~~-~~shall operate the Za-interface.

  Editor' note: Interoperability is a primary issue over the SEG-SEG interface. It may be advantageuos to specify which IP version to use over the Za-interface in order to facilitate interoperability between security domains. This is an **open issue** which SA3 is to consider at SA3#22 (late February 2002).

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

  The Zb-interface is located between SEGs and NEs and between NEs within the same security domain.

  It is for the security domain operator to decide whether and where to deploy Zb-interfaces or not. If deployed, the NEs and SEGs shall be able to use IKE to negotiate, 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-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. It is observed that SEGs are responsible for enforcing security policies towards external destinations and that a combined NE/SEG would have the same responsibility towards external destinations. 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.

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

A.1 Network Address Translators (NATs) and Transition Gateways (TrGWs)

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.

NDS/IP provides no explicit support for Transition Gateways (TrGWs) to be used in the UMTS network domain control plane, but the NDS/IP architecture will not itself prohibit the use of TrGWs. However, the inclusion of TrGWs must be carefully executed in order not to create interoperability problems.

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.

Simple filtering may be needed before the Security Gateway (SEG) functionality. The filtering policy must allow key protocols to allow DNS and NTP etc to pass. This will include traffic over the Za interface from IKE and IPsec ESP in tunnel mode. Unsolicited traffic shall be rejected.

Annex B (normative): Security protection for GTP

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

B.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 protected by NDS/IP mechanisms.

Table 1 presents a list of GTP interfaces that shall be considered by NDS/IP.

Interface	Description	Affected protocol
Gn	Interface between GSNs within the same network	GTP
Gp	Interface between GSNs in different PLMNs.	GTP

Table 1: GTP Interfaces that are affected by NDS/IP

B.2 Policy discrimination of GTP-C and GTP-U

~~SGNs~~ It must be ~~able~~ possible 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, [5]) 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~~ policies shall be checked~~Database (SPD) is consulted~~ for all traffic (both incoming and outgoing) ~~and it processes the datagrams~~ so datagrams can be processed 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-1: 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 the control plane parts of ~~GTP-C for~~ pre-R99 versions of GTP is not possible. Although NDS/IP was not designed for protection of pre-R99 versions of GTP, it is recognized that NDS/IP may also be used for protection of GTP pre-R99. It should be noted that NDS/IP support for pre-R99 versions of GTP is not mandatory.

NOTE-2: NDS/IP has been designed to protect control plane protocols. However, it is recognized that NDS/IP may also be used to protect GTP-U. It should be noted that NDS/IP support for GTP-U is outside the scope of this specification.

B.3 The relationship between BGs and SEGs

It is observed that GPRS Border Gateways (BG) and NDS/IP Security Gateways (SEGs) will both reside at the border of an operator network.

Annex C (normative): Security protection of IMS protocols

~~[Editor's note: According to my noteds we agreed to add a clause to specify the IMS protocol protection.~~

~~Contribution to this clause is wanted!~~]This section details how NDS/IP shall be used to protect IMS protocols and interfaces.

C.1 The need for security protection

The security architecture of the IP multimedia Core Network Subsystem (IMS) is specified in 3G TS 33.203 [10]. This specification, defines that the confidentiality and integrity protection for SIP-signaling is provided in a hop-by-hop fashion.

The first hop i.e. between the UE and the P-CSCF through the IMS access network (i.e. Gm reference point) is protected by security mechanisms specified in [10].

The other hops, within the IMS core network including interfaces within same security domain or between different security domains are protected by NDS/IP security mechanisms as specified by this Technical specification.

TS 23.002 [3] specifies the different reference points defined for IMS.

C.2 Protection of IMS protocols and interfaces

IMS control plane traffic within the IMS core network shall be routed via a SEG when it takes place between different security domains (in particular over those interfaces that may take place between different IMS operator domains such as Mm, Mk, Mg and Sr). In order to do so, IMS operators shall operate NDS/IP Za-interface between SEGs.

It will for the IMS operator to decide whether and where to deploy Zb-interfaces in order to protect the IMS control plane traffic over those IMS interfaces within the same security domain.

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

3GPP TS 33.210 V0.8.0 (2001-12)

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 security is to cover the control signalling on selected interfaces between UMTS network elements.

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 23.002: Network Architecture

[4] 3G TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2

[5] 3G TS 23.228: IP Multimedia (IM) Subsystem - Stage 2

[6] 3G TS 29.060: GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface

[7] 3G TS 33.102: Security Architecture

[8] 3G TS 33.103: Security Integration Guidelines

[9] 3G TS 33.120: Security Objectives and Principles

[10] 3G TS 33.203: Access security for IP-based services

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

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

[13] RFC-2402: IP Authentication Header

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

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

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

[17] RFC-2406: IP Encapsulating Security Payload

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

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

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

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

[22] RFC-2411: IP Security Document Roadmap

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

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

[25] 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.

NDS/IP Traffic: Traffic that requires protection according to the mechanisms defined in this specification.

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
Mm	Interface between a CSCF and an IP multimedia network
Mw	Interface between a CSCF and another CSCF
Za	Interface between SEGs belonging to different networks/security domains
Zb	Interface between SEGs and NEs and interface between NEs within the same network/security domain

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
CSCF	Call State Control Function
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
SIP	Session Initiation Protocol
SPD	Security Policy Database (sometimes also referred to as SPDB)
SPI	Security Parameters Index
TrGW	Transition Gateway

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.

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 [12].

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 NDS/IP traffic shall pass through a SEG before entering or leaving the security domain.

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.

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 the Za-interface, which is located between SEGs from different IP security domains. The IKE and ESP protocols shall 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 protocol Internet Key Exchange (IKE) [18,19,20]. 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 and IKE.

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 (this is the address of the ESP SA endpoint)
- A security protocol identifier (this will always be the ESP protocol in NDS/IP)

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
- There is no need to be able to negotiate SA bundles as only a single ESP SA is set up to protect traffic between the nodes

The IPsec specification of SAs can be found in RFC-2401 [12].

5.2.1 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 or that shall be discarded by 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.

5.2.2 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 shall be automatically created.

5.3 Profiling of IPsec in NDS/IP

This section gives an overview of the features of IPsec that are 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 ESP

When NDS/IP is applied, only the ESP (RFC-2406, [17]) security protocol shall be used for all NDS/IP inter-domain control plane traffic.

5.3.2 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, [12]) is applicable for this case.

The operators may support transport mode to protect communications between NEs within their own network (ie for the Zb-interface).

5.3.3 Support of ESP encryption transforms

IPsec offers a fairly wide set of confidentiality transforms. The transforms that compliant IPsec implementations are required to support are the ESP_NULL and the ESP_DES transforms. However, the Data Encryption Standard (DES) transform is no longer considered to be sufficiently strong in terms of cryptographic strength. This is also noted by IESG in a note in RFC-2407 [18] 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 it shall be mandatory to support the ESP_AES transform.

Editor's Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.

5.3.4 Support of ESP authentication transforms

The transforms that compliant IPsec implementation is required to support are the ESP_NULL, the ESP_HMAC_MD5 and the ESP_HMAC_SHA-1 transforms. For NDS/IP traffic ESP shall always be used to provide integrity, data origin authentication, and anti-replay services, thus the ESP_NULL authentication algorithm is explicitly not allowed for use. ESP shall support ESP_HMAC_SHA-1 and AES MAC algorithms in NDS/IP.

Editor's Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.

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 in CBC mode shall be mandatory for confidentiality
- Support of SHA-1 shall be mandatory for integrity/message authentication

Phase-1 IKE SAs shall be persistent with respect to the IPsec SAs is derived from it. That is, IKE SAs shall have a liftetime for at least the same duration as does the derived IPsec SAs.

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.

Editor's Note: The AES transforms/modes have not yet been finalized; this subclause will be updated when the AES transforms/modes are available.

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. 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 [12,18,19,20] 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 for NDS/IP traffic. The SEGs will then establish and maintain IPsec secured ESP tunnels between security domains. SEGs will normally maintain at least one IPsec tunnel available at all times to a particular peer SEG. The SEG will maintain logically separate SAD and SPD databases for each interface.

The NEs may be able to establish and maintain ESP secured tunnels as needed towards a SEG or other NEs within the same security domain. All NDS/IP 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 between two communicating security domains. 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.This does not preclude negotiation of finer grained security granularity at the discretion of the communicating entities.

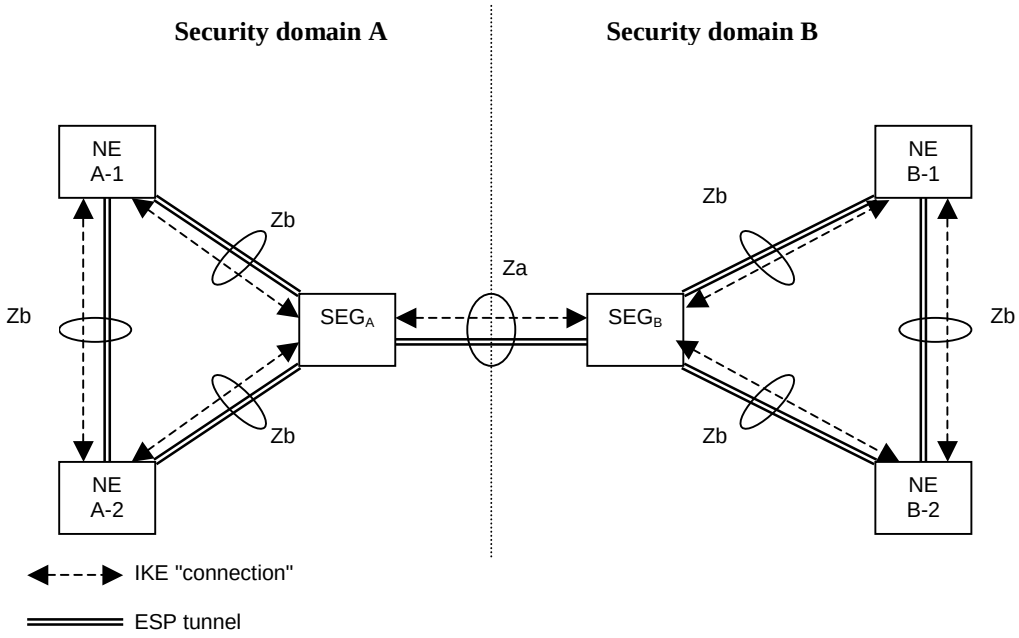

Figure 1: NDS architecture for IP-based protocols

5.6.2 Interface description

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

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

  The Za-interface covers all NDS/IP traffic between security domains. The SEGs uses IKE to negotiate, establish and maintain a secure ESP 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. ESP shall be used with both encryption and authentication/integrity, but an authentictaion/integrity only mode is allowed. The tunnel is subsequently used for forwarding NDS/IP 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.

  All security domains compliant with this specification shall operate the Za-interface.

Editor' note: Interoperability is a primary issue over the SEG-SEG interface. It may be advantageuos to specify which IP version to use over the Za-interface in order to facilitate interoperability between security domains. This is an **open issue** which SA3 is to consider at SA3#22 (late February 2002).

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

  The Zb-interface is located between SEGs and NEs and between NEs within the same security domain.

  It is for the security domain operator to decide whether and where to deploy Zb-interfaces or not. If deployed, the NEs and SEGs shall be able to use IKE to negotiate, 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-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. It is observed that SEGs are responsible for enforcing security policies towards external destinations and that a combined NE/SEG would have the same responsibility towards external destinations. 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.

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

A.1 Network Address Translators (NATs) and Transition Gateways (TrGWs)

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.

NDS/IP provides no explicit support for Transition Gateways (TrGWs) to be used in the UMTS network domain control plane, but the NDS/IP architecture will not itself prohibit the use of TrGWs. However, the inclusion of TrGWs must be carefully executed in order not to create interoperability problems.

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.

Simple filtering may be needed before the Security Gateway (SEG) functionality. The filtering policy must allow key protocols to allow DNS and NTP etc to pass. This will include traffic over the Za interface from IKE and IPsec ESP in tunnel mode. Unsolicited traffic shall be rejected.

Annex B (normative): Security protection for GTP

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

B.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 protected by NDS/IP mechanisms.

Table 1 presents a list of GTP interfaces that shall be considered by NDS/IP.

Interface	Description	Affected protocol
Gn	Interface between GSNs within the same network	GTP
Gp	Interface between GSNs in different PLMNs.	GTP

Table 1: GTP Interfaces that are affected by NDS/IP

B.2 Policy discrimination of GTP-C and GTP-U

It must be possible 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, [5]) IPsec can easily distinguish GTP-C datagrams from other datagrams that may not need IPsec protection.

Security policies shall be checked for all traffic (both incoming and outgoing) so datagrams can be processed 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-1: 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 the control plane parts of pre-R99 versions of GTP is not possible. Although NDS/IP was not designed for protection of pre-R99 versions of GTP, it is recognized that NDS/IP may also be used for protection of GTP pre-R99. It should be noted that NDS/IP support for pre-R99 versions of GTP is not mandatory.

NOTE-2: NDS/IP has been designed to protect control plane protocols. However, it is recognized that NDS/IP may also be used to protect GTP-U. It should be noted that NDS/IP support for GTP-U is outside the scope of this specification.

B.3 The relationship between BGs and SEGs

It is observed that GPRS Border Gateways (BG) and NDS/IP Security Gateways (SEGs) will both reside at the border of an operator network.

Annex C (normative): Security protection of IMS protocols

This section details how NDS/IP shall be used to protect IMS protocols and interfaces.

C.1 The need for security protection

The security architecture of the IP multimedia Core Network Subsystem (IMS) is specified in 3G TS 33.203 [10]. This specification, defines that the confidentiality and integrity protection for SIP-signaling is provided in a hop-by-hop fashion.

The first hop i.e. between the UE and the P-CSCF through the IMS access network (i.e. Gm reference point) is protected by security mechanisms specified in [10].

The other hops, within the IMS core network including interfaces within same security domain or between different security domains are protected by NDS/IP security mechanisms as specified by this Technical specification.

TS 23.002 [3] specifies the different reference points defined for IMS.

C.2 Protection of IMS protocols and interfaces

IMS control plane traffic within the IMS core network shall be routed via a SEG when it takes place between different security domains (in particular over those interfaces that may take place between different IMS operator domains such as Mm, Mk, Mg and Sr). In order to do so, IMS operators shall operate NDS/IP Za-interface between SEGs.

It will for the IMS operator to decide whether and where to deploy Zb-interfaces in order to protect the IMS control plane traffic over those IMS interfaces within the same security domain.

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