ETSI TS 133 210 V10.2.0 (2011-04)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
3G security;
Network Domain Security (NDS);
IP network layer security
(3GPP TS 33.210 version 10.2.0 Release 10)

Reference
RTS/TSGS-0333210va20

Keywords
GSM, LTE, SECURITY, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Definitions, symbols and abbreviations 7
3.1 Definitions 7
3.2 Symbols 8
3.3 Abbreviations 8
4 Overview over network domain security for IP based protocols 9
4.1 Introduction 9
4.2 Protection at the network layer 9
4.3 Security for native IP based protocols 9
4.4 Security domains 10
4.4.1 Security domains and interfaces 10
4.5 Security Gateways (SEGs) 10
5 Key management and distribution architecture for NDS/IP 10
5.1 Security services afforded to the protocols 10
5.2 Security Associations (SAs) 10
5.2.1 Security Policy Database (SPD) 11
5.2.2 Security Association Database (SAD) 11
5.3 Profiling of IPsec 11
5.3.1 Support of ESP 12
5.3.2 Support of tunnel mode 12
5.3.3 Support of ESP encryption transforms 12
5.3.4 Support of ESP authentication transforms 12
5.3.5 Requirements on the construction of the IV 12
5.4 Profiling of IKE 13
5.4.1 Profiling of IKEv1 13
5.4.2 Profiling of IKEv2 13
5.4.3 IKE interoperability 14
5.5 Security policy granularity 14
5.6 Network domain security key management and distribution architecture for native IP based protocols 15
5.6.1 Network domain security architecture outline 15
5.6.2 Interface description 16
Annex A (informative): Other issues 18
A.1 Network Address Translators (NATs) and Transition Gateways (TrGWs) 18
A.2 Filtering routers and firewalls 18
A.3 The relationship between BGs and SEGs 18
Annex B (normative): Security protection for GTP 19
B.1 The need for security protection 19
B.2 Policy discrimination of GTP-C and GTP-U 19
Annex C (normative): Security protection of IMS protocols 21
C.1 The need for security protection 21

C.2 Protection of IMS protocols and interfaces 21

Annex D (normative): Security protection of UTRAN/GERAN IP transport protocols 22

D.1 The need for security protection 22

D.2 Protection of UTRAN/GERAN IP transport protocols and interfaces 22

Annex E (informative): RFC-4303 compared with RFC-2406 23

Annex F (informative): Change history 24

History 25

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 and fixed broadband 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 3GPP and fixed broadband core networks.

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 network domain IP based control planes, which shall be applied to NDS/IP-networks (i.e. 3GPP and fixed broadband networks). The scope of network domain control plane security is to cover the control signalling on selected interfaces between network elements of NDS/IP networks.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 21.133: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements".

[2] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[3] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

[4] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[6] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[7] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[8] 3GPP TS 33.103: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Integration guidelines".

[9] 3GPP TS 33.120: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Principles and Objectives".

[10] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services".

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

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

[13] Void.

[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] Void.

[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".

[26] RFC-3554: "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec".

[27] RFC-1750: "Randomness Recommendations for Security".

[28] 3GPP TS 25.412: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface signalling transport".

[29] RFC-3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec".

[30] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; Authentication Framework".

[31] RFC-4303: "IP Encapsulating Security Payload (ESP)"

[32] RFC-4306: "Internet Key Exchange (IKEv2) Protocol"

[33] RFC-4307: "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)"

[34] RFC-4308: "Cryptographic Suites for IPsec".

[35] RFC-4301: "Security Architecture for the Internet Protocol".

[36] RFC-4835: "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

[37] 3GPP TS 25.422: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iur interface signalling transport".

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.

NDS/IP-networks: 3GPP and fixed broadband networks.

ISAKMP Security Association: A bi-directional logical connection created for security purposes. All traffic traversing a SA is provided the same security protection. The SA itself is a set of parameters to define security protection between two entities.

IPsec Security Association: A unidirectional logical connection created for security purposes. All traffic traversing a SA is provided the same security protection. The SA itself is a set of parameters to define security protection between two entities. A IPsec Security Association includes the cryptographic algorithms, the keys, the duration of the keys, and other parameters.

Security Domain: 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.

Transit Security Domain: A security domain, which is transmitting NDS/IP traffic between other security domains.

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 Session 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
IKEv1	Internet Key Exchange version 1
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPsec	IP security - a collection of protocols and algorithms for IP security incl. key mngt.

ISAKMP	Internet Security Association Key Management Protocol
IV	Initialisation Vector
MAC	Message Authentication Code
NAT	Network Address Translator
NDS	Network Domain Security
NDS/IP	NDS for IP based protocols
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
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TrGW	Transition Gateway

4 Overview over 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 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 network operator or a single transit 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 network domain control plane of an NDS/IP-network 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 network domain security of an NDS/IP-network 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, IP networks.

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

Within a security domain the use of Transport Mode is allowed.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 network domain of an NDS/IP-network 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.

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 NDS/IP 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 points of failure. 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 IKEv1 and IKEv2 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 IPsec security associations. That is, the IPsec SA defines which security protocol to be used, the mode and the endpoints of the SA.

For NDS/IP-networks the IPsec security protocol shall always be ESP. For NDS/IP-networks 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)

For NDS/IP-networks the key management and distribution between SEGs is handled by the protocol Internet Key Exchange (IKEv1) (RFC-2407 [18], RFC-2408 [19] and RFC-2409 [20]) or Internet Key Exchange (IKEv2) (RFC-4306 [32]). The main purpose of IKEv1 and IKEv2 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 IKEv1/IKEv2.

To secure a typical, bi-directional communication between two hosts, or between two security gateways for IKEv1 an ISAKMP Security Associations and two IPsec Security Associations (one in each direction) are required. Similarly when using IKEv2 an IKE SA is established through which the Child Security associations i.e. IPsec security associations are established.

IPsec 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 IPsec security associations in the network domain control plane of NDS/IP-networks the following is noted:

- NDS/IP only requires support for ESP SAs;
- There is no need to be able to negotiate IPsec SA bundles since a single ESP SA is sufficient to set up to protect traffic between the nodes.

The specification of IPsec SAs can be found in RFC-2401 [12] or RFC4301 [35]. The latter reference is the successor of RFC-2401 describing the evolved security architecture.

ISAKMP Security associations as used for IKEv1 are uniquely defined by the following parameters:

- Initiator's cookie;
- Responder's cookie.

With regard to the use of ISAKMP security associations for IKEv1 in the network domain control plane of NDS/IP-networks the following is noted:

- NDS/IP only requires support for ISAKMP SAs with pre-shared keys.

The specification of ISAKMP SAs can be found in RFC-2408 [19].

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

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, the ESP security protocol shall be used IPsec ESP shall be supported either according to RFC-4303 [31] or RFC-2406 [17], however RFC-4303 [31] support is recommended. If RFC-4303 [31] is not supported then RFC-2406[17] shall be supported.

NOTE: Annex E describes the main differences between RFC-4303 [31] and RFC-2406 [17] and the features which require RFC-4303 [31] implementation.

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.

5.3.3 Support of ESP encryption transforms

The implementation conformance requirements for ESP encryption transforms in RFC 4835 [36] shall be followed.

NOTE: These requirements also apply to implementations according to RFC 2407 [18], where a note by IESG warns of future deprecation of the mandatory to support ESP_DES transform.

Only the ESP encryption algorithms mentioned in RFC 4835 [36] shall be used. Algorithms marked with "SHOULD NOT" shall not be used.

5.3.4 Support of ESP authentication transforms

The implementation conformance requirements for ESP authentication transforms in RFC 4835 [36] shall be followed. Algorithms marked with "SHOULD" shall be optional to support.

NOTE: These requirements also apply to implementations according to RFC 2407 [18], where only the HMAC-MD5-96 transform is mandatory to support.

Only the ESP authentication algorithms mentioned in RFC 4835 [36] shall be used. For NDS/IP traffic ESP shall always be used to provide integrity, data origin authentication, and anti-replay services, thus the NULL authentication algorithm is explicitly not allowed for use.

5.3.5 Requirements on the construction of the IV

The following strengthening of the requirements on how to construct the IV shall take precedence over the description given in RFC-2451 [24] section 3 and all other descriptions that allow for predictable IVs.

- The IV field shall be the same size as the block size of the cipher algorithm being used. The IV shall be chosen at random, and shall be unpredictable to any party other than the originator.

- It is explicitly not allowed to construct the IV from the encrypted data of the preceding encryption process.

The common practice of constructing the IV from the encrypted data of the preceding encryption process means that the IV is disclosed before it is used. A predictable IV exposes IPsec to certain attacks irrespective of the strength of the underlying cipher algorithm. The second bullet point forbids this practice in the context of NDS/IP.

These requirements imply that the network elements must have a capability to generate random data. RFC-1750 [27] gives guidelines for hardware and software pseudorandom number generators.

5.4 Profiling of IKE

5.4.1 Profiling of IKEv1

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

For IKEv1 phase-1 (ISAKMP SA):

- The use of pre-shared secrets for authentication shall be supported;
- Only Main Mode shall be used;
- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;
- Support of 3DES in CBC mode shall be mandatory for confidentiality;
- Support of AES in CBC mode (RFC-3602 [29]) shall be mandatory for confidentiality;
- Support of SHA-1 shall be mandatory for integrity/message authentication;
- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange.

Phase-1 IKEv1 SAs shall be persistent with respect to the IPsec SAs is derived from it. That is, IKEv1 SAs shall have a lifetime for at least the same duration as does the derived IPsec SAs.

The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires. The elapsed time between the new SA establishment and the cancellation of the old SA shall be sufficient to avoid losing any data being transmitted within the old SA.

For IKEv1 phase-2 (IPsec SA):

- Perfect Forward Secrecy is optional;
- Only IP addresses or subnet identity types shall be mandatory address types;
- Support of Notifications shall be mandatory;
- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange.

Key Length and support of AES transform:

Since the AES-CBC allows variable key lengths, the Key Length attribute must be specified in both a Phase 1 exchange [20] and a Phase 2 exchange [18]. It is noted that the key length for use with this specification shall be 128 bits.

5.4.2 Profiling of IKEv2

The Internet Key Exchange protocol version may be used for negotiation of IPsec SAs. The following additional requirements on IKEv2 are made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE_SA_INIT exchange:

Following algorithms shall be supported:

- Confidentiality: 3DES in CBC mode;
- Confidentiality: AES in CBC mode (RFC-3602 [29]) with 128-bit key length;
- Pseudo-random function: HMAC-SHA1;
- Integrity: HMAC-SHA1-96;
- Diffie-Hellman group 2 (1024-bit MODP), mandatory for IKEv2 according to ref. [33].

- Diffie-Hellman group 14 (2048-bit MODP), recommended for IKEv2 according to ref. [33].

For security reasons, the use of Diffie-Hellman group 2 (1024-bit MODP) is not recommended. If a larger group is available, it should be used.

Following algorithms should be supported:

- Pseudo-random function: AES-XCBC-PRF-128;
- Integrity: AES-XCBC-MAC-96.

For IKE_AUTH exchange:

- The use of pre-shared secrets for authentication shall be supported;
- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;
- Re-keying of IPsec SAs and IKE SAs shall be supported as specified in [32].

For the CREATE_CHILD_SA exchange:

- Perfect Forward Secrecy is optional.

5.4.3 IKE interoperability

Although both IKE versions have a lot of features and functionality in common, IKEv1 is not interoperable with IKEv2. Therefore, this clause lists the necessary IKE requirements in order to ensure proper interoperability between the different NDS/IP nodes in order to set up the needed security associations for the Za and Zb-interfaces.

SEGs shall implement both IKEv1and IKEv2. This ensures that a common version of the Internet Key Exchange Protocol is always supported on Za interface between any two SEGs. Consequently, a hop-by-hop protection is always possible on the path NE-SEG-SEG-NE using one of the two Internet Key Exchange protocols

NOTE 1: A SEG compliant with this specification may have to communicate with a SEG compliant to a former 3GPP Release. In this case the 3GPP standards ensure interoperability between these two SEGs by using IKEv1 to establish the required security associations.

If both IKEv2 and IKEv1 are available on the Za-interface then IKEv2 shall be used.

For the Zb-interface, NEs shall implement either IKEv1 or IKEv2, but may also implement both IKE versions.

NOTE 2: A SEG compliant with this specification may have to communicate with an NE which is compliant to a former 3GPP Release over the Zb interface. In this case the 3GPP standards ensure interoperability between them by using IKEv1 to establish the required security associations.

NOTE 3: As the use of IKEv2 has certain security and performance advantages over IKEv1, the use of IKEv2 in new NEs is encouraged.

If both IKEv2 and IKEv1 are available on the Zb-interface then IKEv2 shall be used.

When using Internet Keying Exchange protocol to establish the needed security associations for the Zb-interface between two NEs in the same security domain, it may be possible that no common version of IKE is supported. In this case the use of an intermediate SEG which is compliant to this specification will enable the two NEs to interoperate by establishing the necessary secured connectivity between them.

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 Security Association between the NEs or SEGs. The normal mode of operation is that only one ESP Security Association 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-security domain policy is determined by roaming

agreements when the security domains belong to different operators or may be unilaterally decided by the operator when the security domains both belong to him. IPsec security policy enforcement for inter-security domain communication is a matter for the SEGs of the communicating security domains.

5.6 Network domain security 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 IKEv1 protocol (RFC-2401 [12], RFC-2407 [18], RFC-2408 [19], RFC-2409 [20] or IKEv2 RFC-4306 [32]) 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. Sections 5.3 and 5.4 give an overview over the profiling of IPsec and IKEv1/IKEv2 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 Security Association in tunnel mode 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 Security Associations 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 be afforded hop-by-hop security protection towards the final destination.

Operators may decide to establish only one ESP Security Association 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.

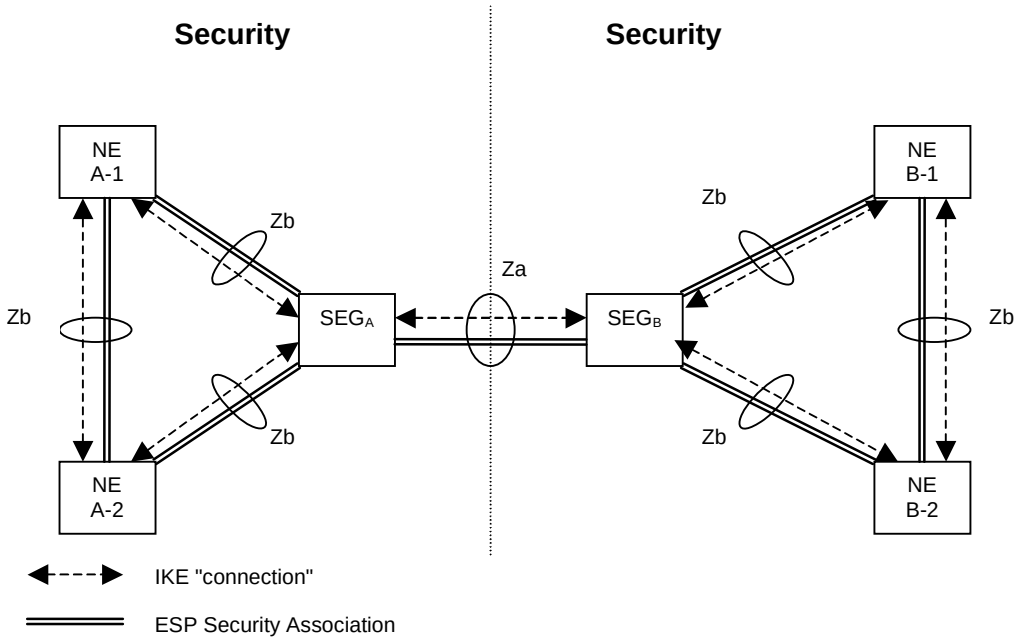

Figure 1: NDS architecture for IP-based protocols

Additional guidelines on how to apply IPsec in SCTP are specified in RFC3554 [26]. This RFC is optional for implementation unless otherwise explicitly indicated per reference point.

NOTE: TS 33.310 [30] defines an inter-operator Public Key Infrastructure (PKI) that can be used to support the establishment of IPsec connections.

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. On the Za-interface, authentication/integrity protection is mandatory and encryption is recommended. ESP shall be used for providing authentication/integrity protection and encryption. The SEGs use IKEv1 or IKEv2 to negotiate, establish and maintain a secure ESP tunnel between them. The tunnel is subsequently used for forwarding NDS/IP traffic between security domain A and security domain B. Inter-SEG tunnels can be available at all times, but they can also be established as needed.

  One SEG of security domain A can be dedicated to only serve a certain subset of security domains that security domain A needs to communicate with. 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.

NOTE 1: It is possible to use transit security domains between other security domains. The Za interface is used to protect the interface between the transit security domain and other security domains. If there are multiple transit security domains between two security domains then Za-interface is used to protect interfaces between transit security domains.

NOTE 2: Further details about the usage of encryption in specific cases are provided in the (normative) Annexes of the present document and in other 3GPP specifications referencing the present document.

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

  The Zb-interface is located between SEGs and NEs and between NEs within the same security domain. The Zb-interface is optional for implementation. If implemented, it shall implement ESP in tunnel mode and at least one of the IKE versions described in clause 5.4. The support of ESP in Transport mode is optional.

On the Zb-interface, ESP shall always be used with authentication/integrity protection. The use of encryption is optional. The ESP Security Association shall be used for all control plane traffic that needs security protection.

Whether the Security Association is established when needed or a priori is for the security domain operator to decide. The Security Association is subsequently used for exchange of NDS/IP traffic between the NEs.

NOTE 3: The security policy established over the Za-interface may be 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 4: 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 to have secure direct inter-domain NE←→NE communication within the framework of NDS/IP if both NEs have implemented SEG functionality. If a NE and SEG is combined in one physical entity, the SEG functionality of the combined unit should not be used by other NEs towards external security domains.

Annex A (informative): Other issues

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

Network Address Translators (NATs) are not designed to be part of the network domain control plane of NDS/IP-networks. 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 network domain control plane of NDS/IP-networks, 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 IKEv1/IKEv2 and IPsec ESP in tunnel mode. Unsolicited traffic shall be rejected.

A.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 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 3GPP TS 29.060 [6]. 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.

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

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

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 [6]) 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.

Annex C (normative): Security protection of IMS protocols

This section details how NDS/IP shall be used to protect IMS protocols and interfaces. The network domain security for IMS in 3GPP2 networks shall be as specified in in Annex S.5 of TS 33.203[10].

C.1 The need for security protection

The security architecture of the IP multimedia Core Network Subsystem (IMS) is specified in 3GPP TS 33.203 [10]. 3GPP TS 33.203 [10] defines that the confidentiality and integrity protection for SIP-signalling are 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 3GPP TS 33.203 [10].

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

3GPP 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 exist between different IMS operator domains). In order to do so, IMS operators shall operate NDS/IP Za-interface between SEGs as described in clause 5.6.2.

When SEGs are deployed to secure a Za reference point potentially carrying IMS session keys (i.e. in IMS roaming scenarios, when SEGs are deployed between a P-CSCF and I-CSCF located in different security domains), IPSec ESP shall be used with both encryption and integrity protection for all SIP signalling traversing inter-security domain boundaries.

It will be 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 (normative): Security protection of UTRAN/GERAN IP transport protocols

This annex details how NDS/IP shall be used to protect UTRAN/GERAN IP transport protocols and interfaces.

D.1 The need for security protection

The control plane in question is used to transfer signalling messages in UTRAN/GERAN IP transport network. The UTRAN IP transport option is specified in Rel5 UTRAN Technical Specifications. UTRAN Iu interface signalling transport is specified in 3GPP TS 25.412 [28] and Iur interface signalling transport in TS 25.422 [37]. Based on the known security threats in IP networking, the traffic shall be protected properly. This is in order not to restrict the application of IP in UTRAN and GERAN only to closed network environments.

The security solution for IP based UTRAN/GERAN transport shall follow the principles introduced in the NDS/IP since the IPSec provides application independent security solution for all IP traffic.

Iu and Iur interfaces are carrying information that is classified as sensitive. Iu and Iur are used for conveying e.g. subscriber specific security keys. These keys are vital for the end-user security. Hence Iu and Iur shall be encrypted along with the integrity check.

D.2 Protection of UTRAN/GERAN IP transport protocols and interfaces

IPSec ESP shall be used with both encryption and integrity protection for all RANAP and RNSAP messages traversing inter-security domain boundaries.

Iu and Iur control plane traffic shall be routed via a SEG when it takes place between different security domains (in particular over those interfaces that may exist between different operator domains). In order to do so, operators shall operate NDS/IP Za-interface between SEGs. If a UTRAN node has implemented SEG functionality within the same physical entity, transport mode IPsec is optional for implementation and use on the Iur interface.

It will be for the operator to decide whether and where to deploy Zb-interfaces in order to protect the RANAP and RNSAP messages over the Iu and Iur interfaces within the same security domain.

Annex E (informative): RFC-4303 compared with RFC-2406

If none of the new features available in RFC-4303[31] are employed, then the format of an ESP packet is identical to the format of those packets which are generated following RFC-2406[17]. RFC-4303[31] provides a detailed description.

The new features of RFC-4303 [31] that affect the format are:

1) Use of combined mode encryption algorithm

However, a peer who implements only RFC-2406 [17] would never negotiate such an algorithm, as they are defined for use only in RFC-4303 [31].

2) ESN (Extended Sequence Numbering)

This feature requires an extension to IKEv1 in order to be able to negotiate it and can be negotiated through IKEv2. This feature is useful for very high bandwidth environments.

3) Better support of traffic flow confidentiality (TFC) in RFC-4303 [31].

NOTE 1: RFC-4303 [31] section 8 describes how an RFC-2406 [17] receiver needs to behave when receiving an ESP packet with the Next Header field set to a value of "59".

NOTE: The implementation of RFC-4303 [31] is functionally required if IPsec multicast needs to be supported on an interface.

Annex F (informative): Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WI**
03-2002	SA_15	SP-020117	-	-	Approved at TSG SA#15 and placed under change control	2.0.0	5.0.0	
06-2002	SA_16	SP-020355	0001		NDS/IP Confidentiality protection for IMS session keys	5.0.0	5.1.0	
06-2002	SA_16	SP-020356	0002		Strengthening the requirements on IV construction to prevent attacks based on predictable IV	5.0.0	5.1.0	
12-2002	SA_18	SP-020719	0003		Adding requirement to provide mandatory support for 3DES encryption in NDS/IP.Remove AES references and dependencies	5.1.0	5.2.0	
12-2002	SA_18	SP-020720	0004		Securing UTRAN/GERAN IP Transport interfaces and specifically the Iu interface with NDS/IP mechanisms (Implemented after Rel-5 CR 003 included)	5.1.0	6.0.0	SECNDSIP
03-2003	SA_19	SP-030104	0006		Za-interface and roaming agreements	6.0.0	6.1.0	SECNDSIP
03-2003	SA_19	SP-030105	0008		Clarification to the re-keying aspects of network domain security	6.0.0	6.1.0	SECNDSIP
06-2003	SA_20	SP-030225	0010		Use of IPsec ESP with encryption on the Za-interface	6.1.0	6.2.0	SECNDSIP
09-2003	SA_21	SP-030488	0012		Change of IKE profiling	6.2.0	6.3.0	SECNDSIP
09-2003	SA_21	SP-030489	0014		Update draft-ietf-ipsec-sctp-04.txt reference to new standard RFC: RFC 3554	6.2.0	6.3.0	SECNDSIP
03-2004	SA_23	SP-040153	0015	-	Addition of AES transform	6.3.0	6.4.0	SECNDSIP
06-2004	SA_24	SP-040374	0016	-	Diffie-Hellman groups in NDS/IP	6.4.0	6.5.0	SEC-NDS-IP
2005-12	SP- 30	SP-050841	0017	2	Extension of scope to encompass TISPAN NGN	6.5.0	7.0.0	FBI
2006-09	SP-33	SP-060492	0019	-	Clarifying the use of RFC3554	7.0.0	7.1.0	SEC1-NDS
2006-12	SP-34	SP-060808	0020	1	Clarifying the use of transit security domains	7.1.0	7.2.0	SEC7-NDS
2006-12	SP-34	SP-060808	0021	1	Addition of reference to NDS/AF specification	7.1.0	7.2.0	SEC7-NDS
2007-09	SP-37	SP-070590	0022	1	Clarification on the use of the IPSec mode for the Zb-reference point	7.2.0	7.3.0	SEC1-NDS
2008-03	SP-39	SP-080142	0024	-	Introducing the support of IKEv2 for EPS	7.3.0	8.0.0	SAES
2008-03	SP-39	SP-080142	0025	1	Introducing the support of RFC-4303 for EPS	7.3.0	8.0.0	SAES
2008-09	SP-41	SP-080544	0023	3	Introduction of Network Domain Security support for 3GPP2 IMS	8.0.0	8.1.0	IMS-Sec
2008-12	SP-42	SP-080747	0026	-	Update of IKEv2 SA profile	8.1.0	8.2.0	TEI8
2009-06	SP-44	SP-090273	0027	--	Clarification about the encryption on Za reference point	8.2.0	8.3.0	TEI8
2009-12	-	-	-	-	Update to Rel-9 version (MCC)	8.3.0	9.0.0	-
2010-06	SP-48	SP-100251	0028	-	Correction of explanations of abbreviations CSCF and IKEvx	9.0.0	9.1.0	TEI9
2010-10	SP-49	SP-100	0029	2	IPsec Alignment	9.1.0	10.0.0	TEI10
2010-10	SP-49	SP-100	0031	-	Clarification on usage of ESP authentication and encryption transforms	9.1.0	10.0.0	TEI10
2010-12	SP-50	SP-100731	0033	-	NDS corrections	10.0.0	10.1.0	TEI10
2011-03	SP-51	SP-110019	0036	1	Correction of Iur security	10.1.0	10.2.0	TEI10

History

Document history		
V10.2.0	April 2011	Publication