ETSI TS 133 210 V15.2.2 (2019-10)

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
3G security;
Network Domain Security (NDS);
IP network layer security
(3GPP TS 33.210 version 15.2.2 Release 15)

Reference
RTS/TSGS-0333210vf22

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 5
Introduction 5
1 Scope 6
2 References 6
3 Definitions, symbols and abbreviations 8
3.1 Definitions 8
3.2 Symbols 9
3.3 Abbreviations 9
4 Overview over network domain security for IP based protocols 10
4.1 Introduction 10
4.2 Protection at the network layer 10
4.3 Security for native IP based protocols 10
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 11
5.1 Security services afforded to the protocols 11
5.2 Security Associations (SAs) 11
5.2.0 General 11
5.2.1 Security Policy Database (SPD) 12
5.2.2 Security Association Database (SAD) 12
5.3 Profiling of IPsec 12
5.3.0 General 12
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 13
5.3.5 Requirements on the construction of the IV 13
5.4 Profiling of IKEv2 13
5.4.0 General 13
5.4.1 Void 13
5.4.2 Profiling of IKEv2 13
5.4.3 Void 14
5.5 Security policy granularity 15
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
6 Other 3GPP profiles 17
6.1 General 17
6.2 TLS protocol profiles 17
6.2.1 General 17
6.2.2 Profiling for TLS 1.3 18
6.2.3 Profiling for TLS 1.2 and earlier 18
6.3 JWE and JWS profiles 19
6.3.1 General 19
6.3.2 JWE profile 20
6.3.3 JWS profile 20
Annex A (informative): Other issues 21

A.1 Network Address Translators (NATs) and Transition Gateways (TrGWs) 21
A.2 Filtering routers and firewalls 21
A.3 The relationship between BGs and SEGs....21

Annex B (normative): Security protection for GTP 22
B.0 General 22
B.1 The need for security protection....22
B.2 Policy discrimination of GTP-C and GTP-U 22
B.3 Protection of GTP-C transport protocols and interfaces 23

Annex C (normative): Security protection of IMS protocols 24
C.0 General 24
C.1 The need for security protection....24
C.2 Protection of IMS protocols and interfaces 24

Annex D (normative): Security protection of UTRAN/GERAN IP transport protocols....25
D.0 General 25
D.1 The need for security protection....25
D.2 Protection of UTRAN/GERAN IP transport protocols and interfaces....25

Annex E (informative): RFC-4303 compared with RFC-2406....26

Annex F (informative): Change history 27
History 29

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 GPRS systems is the absence of security in the core network. This was formerly perceived not to be a problem, since the GPRS 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 UMTS 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.

Starting with LTE, but especially with 5G, security of signalling protocols moves onto the application layer. The current document is the central repository of the protection mechanisms and profiles for these protocols.

This document 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. . The present document furthermore serves as a central repository for cryptographic profiles for security above IP layer.

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] -[25] Void.

[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] Void.

[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] Void.

[33] Void

[34] Void.

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

[36] Void.

[37] Void.

[38] 3GPP TS 25.422: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iur interface signalling transport".

[39] 3GPP TS 25.467: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN architecture for 3G Home Node B (HNB); Stage 2".

[40] 3GPP TS 25.468: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh Interface RANAP User Adaption (RUA) signalling".

[41] 3GPP TS 25.471: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iurh Interface RNSAP User Adaption (RNA) signalling".

[42] RFC-6311: "Protocol Support for High Availability of IKEv2/IPsec".

[43] RFC-7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[44] IANA: "Internet Key Exchange Version 2 (IKEv2) Parameters".

[45] RFC-7321: "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

[46] IETF RFC 7515: "JSON Web Signature (JWS)".

[47] IETF RFC 7516: "JSON Web Encryption (JWE)".

[48] IETF RFC 7518: "JSON Web Algorithms (JWA)".

[49] IETF RFC 6347: "Datagram Transport Layer Security Version 1.2".

[50] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[51] IETF RFC 8442: "ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites for TLS 1.2 and DTLS 1.2”.

[52] IETF RFC 2818: "HTTP Over TLS".

[53] IETF RFC 2817: "Upgrading to TLS Within HTTP/1.1".

[54] IETF RFC 5288: "AES Galois Counter Mode (GCM) Cipher Suites for TLS".

[55] IETF RFC 5289: "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)".

[56] IETF RFC 4492: "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)".

[57] IETF RFC 6066: "Transport Layer Security (TLS) Extensions: Extension Definitions".

[58] IETF RFC 4366: "Transport Layer Security (TLS) Extensions".

[59] IETF RFC 5077: "Transport Layer Security (TLS) Session Resumption without Server-Side State".

[60] IETF RFC 5746: "Transport Layer Security (TLS) Renegotiation Indication Extension".

[61] IETF RFC 7627: "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension".

[62] IETF RFC 7919: "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)".

[63] IETF RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[64] IETF RFC 5489: "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)".

[65] IETF RFC 5487: "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode".

[66] IETF RFC 8446: “The Transport Layer Security (TLS) Protocol Version 1.3".

[67] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

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.

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
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-4301 [35] and 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