ETSI TS 187 003 V2.1.1 (2009-02)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture

Reference

RTS/TISPAN-07029-NGN-R2

Keywords

architecture, security

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

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 Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document defines the security architecture of NGN. The definition complies with the requirements of ITU-T Recommendation I.130 [29] at stage 2.

The present document addresses the security architecture required to fulfil the NGN security requirements defined in TS 187 001 [1] and includes the definition of security architectures to provide protection for each of the NGN functional architecture (ES 282 001 [2]) and its subsystems (ES 282 004 [5], ES 282 001 [3], ES 282 007 [24], ES 283 003 [23] and ES 282 003 [4]). Where appropriate the present document endorses security mechanisms defined in other specifications.

The present document addresses the security issues of the NGN core network and the NGN access network(s) up to and including the NGN Network Termination (NGN NT) in the residential customer domain. The NGN NT denotes a logical demarcation point between the residential customer domain and the NGN core and access networks and covers the corresponding interfaces.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[2] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[3] ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[4] ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture".

[5] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[6] ETSI TS 183 033: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia; Diameter based protocol for the interfaces between the Call Session Control Function and the User Profile Server Function/Subscription Locator Function; Signalling flows and protocol details [3GPP TS 29.228 V6.8.0 and 3GPP TS 29.229 V6.6.0, modified]".

[7] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)".

[8] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

[9] ETSI TS 133 141: "Universal Mobile Telecommunications System (UMTS); Presence service; Security (3GPP TS 33.141)".

[10] ETSI TS 133 222: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (3GPP TS 33.222)".

[11] ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220)".

[12] ETSI TS 122 048: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Security Mechanisms for the (U)SIM application toolkit; Stage 1 (3GPP TS 22.048)".

[13] ETSI TS 123 048: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Security mechanisms for the (U)SIM application toolkit; Stage 2 (3GPP TS 23.048)".

[14] ETSI TS 131 101: "Universal Mobile Telecommunications System (UMTS); UICC-terminal interface; Physical and logical characteristics (3GPP TS 31.101)".

[15] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102)".

[16] ETSI TS 131 103: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Characteristics of the IP Multimedia Services Identity Module (ISIM) application (3GPP TS 31.103)".

[17] ETSI TS 129 329: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329)".

[18] ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Subsystem (PES); NGN Release 1 H.248 Profile for controlling Access and Residential Gateways".

[19] ETSI ES 283 018: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification".

[20] ETSI TS 183 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; Network Access xDSL and WLAN Access Networks; Interface Protocol Definitions".

[21] ETSI ES 283 035: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".

[22] ETSI ES 283 034: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol".

[23] ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3".

[24] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[25] ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 v7.2.0, modified)".

[26] IETF RFC 3261: "SIP: Session Initiation Protocol".

[27] ISO/IEC 10181-1 (1996): "Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview".

[28] ISO/IEC 11770-1 (1996): "Information technology - Security techniques - Key management - Part 1: Framework".

[29] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[30] ITU-T Recommendation X.810 (1995): "Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview".

[31] ITU-T Recommendation X.811: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Authentication framework".

[32] ITU-T Recommendation X.812: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Access control framework".

[33] ITU-T Recommendation X.814: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Confidentiality framework".

[34] ITU-T Recommendation X.815: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Integrity framework".

[35] ETSI TS 183 017: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification".

[36] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[37] ETSI TS 183 043: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation; Stage 3 specification".

[38] ETSI TS 182 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

[39] ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102)".

[40] ETSI ES 283 026: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification".

[41] ETSI ES 202 238: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Evaluation criteria for cryptographic algorithms".

[42] IEEE 802.1x: "Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control".

[43] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Service and Capability Requirements".

[44] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[45] ETSI TS 123 002: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Network architecture".

[46] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TR 133 919: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G Security; Generic Authentication Architecture (GAA); System description (3GPP TR 33.919)".

[i.2] ETSI TR 133 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Support for subscriber certificates (3GPP TS 33.221)".

[i.3] ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

[i.4] ETSI TR 183 032: "Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Feasibility study into mechanisms for the support of encapsulated ISUP information in IMS".

[i.5] ETSI TR 182 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Organization of user data".

[i.6] ETSI TR 183 014: "Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Development and Verification of PSTN/ISDN Emulation".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

AUTHentication service (AUTH): See ITU-T Recommendation X.811 [31].

AUTHORization service (AUTHOR): See ITU-T Recommendation X.812 [32].

CONFidentiality service (CONF): See ITU-T Recommendation X.814 [33].

content protection: protection of content (files or streams) post-delivery

NOTE: It ensures that a user can only use the content in accordance with the license that they have been granted, e.g. play/view/hear multiple times or hours, etc.

data: any information conveyed in communication packets as well as any other information such as topology information

INTegrity service (INT): See ITU-T Recommendation X.815 [34].

Key Management service (KM): See ISO/IEC 11770-1 [28].

license: data package which represents the granted Rights to a specific user and the key related to the protected content

NGN Network Termination (NGN NT): reference point which denotes a logical demarcation point between the residential customer domain and the NGN core via access networks

NOTE: It covers the corresponding interfaces.

Policy Enforcement Function (PEF): security function that enforces policy rules

NOTE: The PEF encompasses functions for filtering and topology hiding such as typically found in firewalls and/or session border controllers.

rights: pre-defined set of usage entitlement to the content

NOTE: The entitlement may include the permissions (e.g. to view/hear, copy, modify, record, distribute, etc.), constraints (e.g. play/view/hear multiple times or hours), etc.

security domain: set of elements made of security policy, security authority and set of security relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain

NOTE: The activities of a security domain involve one or more elements from that security domain and, possibly, elements of other security domains

service protection: protection of content (data or media stream) during the delivery time or the time of transmission

3.2 Abbreviations

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

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization, Accounting
ACK	ACKnowledge
ACR	Anonymous Communications Rejection
AF	Application Functions
AGCF	Access Gateway Control Function
AGW	Access GateWay
AKA	Authentication and Key Agreement
AMF	Access Management Function
AN	Access Network
AN	Access Node
AP	Access Point
AP	Authentication Proxy
A-RACF	Access-Resource Admission Control Function
ARF	Access Relay Function
AS	Application Server
ASP	Application Service Provider
AuC	Authentication Centre
AUTH	AUTHentication service
AUTHOR	AUTHORization service
AUTN	AUthentication TokeN
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
BSF	Bootstrapping Server Functionality
CA	Certification Authority

C-BGF	Core Border Gateway Function
CEF	Content Encryption Function
CLF	Connectivity session and repository Location Function
CNG	Customer Network Gateway
CONF	CONFidentiality service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSCF	Call Session Control Function
DoS	Denial-of-Service
DRM	Digital Rights Management
ESP	Encapsulating Security Protocol
FE	Functional Entity
FFS	For Further Study
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GE	Generic Entities
GRE	Generic Routing Encapsulation
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	HyperText Transport Protocol
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
I-CSCF	Interrogating Call Session Control Function
ID	IDentity
IETF	Internet Engineering Task Force
IF	InterFace
IKE	Internet Key Exchange
IMPI	IMS Private User ID
IMPU	IMS Public User ID
IMS	IP Multimedia Subsystem
INT	INTegrity service
INTF	INTegrity Function
IP	Internet Protocol
IPsec	Internet Protocol security
IPTV	Internet Protocol TeleVision
IRG	IMS Residential Gateway
ISIM	IMS Subscriber Identity Module
ISUP	ISDN User Part
IUA	ISDN Q.921-User Adaptation
KM	Key Management service
KMF	Key Management Function
LIF	Licensing Issuing Function
MAA	Multimedia Auth Answer
MDF	Media Delivery Function
ME	Mobile Equipment
MGC	Media Gateway Controller
MGCF	Media Gateway Control Function
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
n.a.	not applicable
NACF	Network Access Configuration Function
NAF	Network Application Function
NAPT	Network Address and Port Translation
NASS	Network Access SubSystem
NAT	Network Address Translation
NBA	NASS Bundled Authentication
NDS	Network Domain Security
NE	Network Element
NGN NT	NGN Network Termination
NGN	Next Generation Network
OIR	Originating Identity Presentation
P-CSCF	Proxy Call Session Control Function

PDBF	Profile DataBase Function
PEF	Policy Enforcement Function
PES	PSTN/ISDN Emulation
PS	Packet Switched
RACS	Resource Admission Control Subsystem
RAND	RANDom
RGW	Residential GateWay
SA	Security Association
SCF	Service Control Function
SCS	OSA Service Capability Server
S-CSCF	Serving Call Session Control Function
SDO	Standards Development Organisation
SDP	Session Description Protocol
SEG	Security Gateway
SEGF	SEcurity Gateway Function
SGF	Signalling Gateway Function
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SPD	Security Policy Database
SPDF	Service Policy Decision Function
SSC	Support for Subscriber Certificates
SSF	Service Selection Function
TE	Terminal Equipment
THF	Topology Hiding Function
THIG	Topology Hiding Interconnection Gateway
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TLS	Transport Layer Security
T-MGF	Trunking Media Gateway Function
TS	Technical Specification
UA	User Agent
UAAF	User Access Authorization Function
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UPSF	User Profile Server Function
URI	Uniform Resource Identifier
USIM	UMTS Subscriber Identity Module
VGW	Voice over IP GateWay
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol
XML	eXtensible Markup Language

4 NGN Security

This clause provides an overview of the NGN security document. The entire document can be seen as a documented output of a security process that loops through several stages; see figure 1, where arrows indicate logical steps and dependencies.

The present document assumes existence of a well-defined NGN architecture (see ES 282 001 [2]) that includes the IMS architecture (TS 123 002 [45]), the Network Attachment Subsystem (NASS) architecture (see ES 282 004 [5], the Resource Admission Subsystem (RACS) architecture (see ES 282 003 [4]), and the PSTN/ISDN Emulation (PES) architecture (see ES 282 002 [3]). Likewise, the present document assumes the corresponding IMS security architecture (seeTS 133 102 [39]). IMS architecture and IMS security architecture are shown as dashed boxes; those prerequisites are not specified further in the present document.

The description of the NGN security architecture has been divided in a number of smaller blocks describing the security interfaces, the security functions and security protocols, security building blocks and security components.

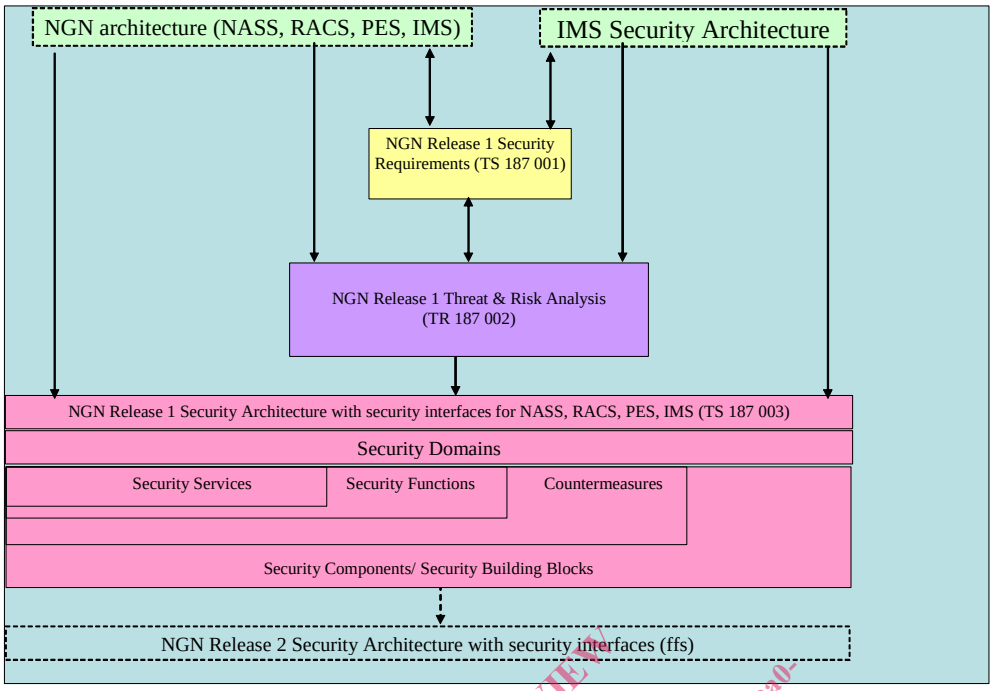

Figure 1: Overview of NGN security documents

4.1 NGN security architecture

The NGN security architecture basically consists of the following major parts:

- NGN security domains (see clause 4.3).
- Security services (see clause 5):
  - authentication;
  - authorization;
  - policy enforcement;
  - key management;
  - confidentiality; and
  - integrity.
- Security protocols including those contained in:
  - IMS Access Security (see TS 133 203[7]);
  - SIP HTTP-digest (see RFC 3261 [26]) (for NGN legacy UE);
  - XCAP (see TS 183 033[6]), presence security (see TS 133 141[9]).
- Application specific key management.
- SEGFs to secure signalling and control communication among network entities/FEs. Security Gateways (SEGs) for IMS network domain security - as defined by TS 133 210 [8] - are considered primarily functional components. The present document endorses SEGs and calls them **Security Gateway Function (SEGF)**.
- IMS Residential Gateway to secure access of legacy UEs (see clause 6).