

ETSI TS 187 003 V3.4.1 (2011-03)

Technical Specification

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

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 187 003 V3.4.1 \(2011-03\)](https://standards.iteh.ai/catalog/standards/etsi/a1df5ba5-0c97-4078-8cb1-ff92ee19fbe4/etsi-ts-187-003-v3-4-1-2011-03)

<https://standards.iteh.ai/catalog/standards/etsi/a1df5ba5-0c97-4078-8cb1-ff92ee19fbe4/etsi-ts-187-003-v3-4-1-2011-03>



Reference

RTS/TISPAN-07038-NGN-R3

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

(<https://standards.iteh.ai>)
Document Preview

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/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE™ is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	5
Foreword.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	8
3 Definitions and abbreviations.....	9
3.1 Definitions.....	9
3.2 Abbreviations	9
4 NGN Security	12
4.0 Overview	12
4.0a Security services identified in TS 187 001 and TR 187 002	12
4.1 NGN security architecture.....	13
4.2 Security domains	17
4.3 Void.....	18
4.4 Void.....	18
4.5 PES Security Architecture.....	18
4.5.1 Security for H.248 within PES.....	18
4.6 Application security architecture.....	19
4.6.1 Generic Authentication Architecture (GAA).....	19
4.6.1.1 Generic Bootstrapping Architecture (GBA).....	20
4.6.1.2 Support for Subscriber Certificates (SSC)	20
4.6.1.3 Access to NAF using HTTPS.....	20
4.6.2 HTTP Digest authentication for UICC-less CNDs	20
5 Void.....	22
6 Void.....	22
7 Void.....	22
7.1 Void.....	22
7.2 Void.....	22
8 Void.....	22
9 Security Architectures for IPTV.....	22
9.1 Content Protection.....	22
9.1.2 Reference Points	23
9.1.2.1 LIF – UE (s-cp-1).....	23
9.1.2.2 KMF – LIF (s-cp-2)	23
9.1.2.3 KMF – CEF (s-cp-3)	23
9.1.2.4 CEF – MDF (s-cp-4)	24
9.2 Service Protection.....	24
9.3 Optional solutions.....	24
9.3.1 Any Content Protection	24
9.3.1.1 Reference Points	25
9.3.1.2 Procedures	25
9.3.1.2.1 Content Preparation	25
9.3.1.2.2 Content Delivery	25
9.3.1.2.3 Right and Key Delivery	25
9.3.2 OMA BCAST	25
9.3.2.1 OMA BCAST Functional Architecture.....	26
9.3.2.2 Mapping between TISPAN IPTV Architecture and OMA BCAST Service Protection Functional Architecture.....	27
9.3.2.3 Mapping between TISPAN IPTV Service Protection based on 4-layer Key Hierarchy and OMA BCAST Service Protection Functional Architecture.....	29

9.3.2.4	OMA BCAST Smart Card Profile adaptation to MPEG-2 TS	30
9.3.2.4.1	STKM Transport in MPEG-2 TS	30
9.3.2.4.2	STKM and MPEG-2 TS encryption	32
10	Void	33
11	Void	33
12	Void	33
12.1	Void	33
12.2	Void	33
13	Security Architecture for Corporate Networks	33
13.1	Subscription Based Business Trunking	33
13.2	Peering Based Business Trunking	33
14	Security Architecture for Host Enterprise	33
Annex A (informative): NGN-relevant security interfaces		34
A.1	Network attachment security interfaces	34
A.1.1	Reference Point e1 (CNG - AMF)	35
A.1.2	Reference Point e2 (CLF - AF)	35
A.1.3	Reference Point a3 (AMF - UAAF)	35
A.1.4	Reference Point e5 (UAAF - UAAF)	35
A.2	Service layer security interfaces	36
A.2.1	NGN IP Multimedia Subsystem (IMS)	36
A.2.1.1	Reference Point Gm (UE - P-CSCF)	36
A.2.1.2	Reference Point Cx (CSCF - UPSE)	37
A.2.1.3	Reference Point Gq' (P-CSCF - RACS)	37
A.2.1.4	Reference Point Iw (IWF - non-compatible SIP)	37
A.2.1.5	Reference Point Ic (IBCF - IMS)	37
A.2.1.6	Void	37
A.2.1.7	Reference Point Ut (UE - AS)	37
A.3	Interconnection security interfaces	38
A.3.1	Interconnecting security at the transport layer	39
A.3.2	Interconnecting security at the service layer	39
Annex B (informative): Mapping of NGN Security Requirements to Security Services		40
Annex C: Void		46
Annex D: Void		47
Annex E (informative): Open Issues in NGN Security		48
Annex F: Void		49
Annex G (informative): Bibliography		50
Annex H (informative): Change history		52
History		53

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).

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TS 187 003 V3.4.1 \(2011-03\)](https://standards.iteh.ai/catalog/standards/etsi/a1df5ba5-0c97-4078-8cb1-ff92ee19fbe4/etsi-ts-187-003-v3-4-1-2011-03)

<https://standards.iteh.ai/catalog/standards/etsi/a1df5ba5-0c97-4078-8cb1-ff92ee19fbe4/etsi-ts-187-003-v3-4-1-2011-03>

1 Scope

The present document defines the security architecture of NGN.

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 (NASS ES 282 004 [5], PES ES 282 002 [3], ES 282 007 [15], SIP and SDP call control ES 283 003 [14] and RACS 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) and the Customer Premises network (CPN).

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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 necessary for the application of the present document.

- [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); LTE; 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); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".
- [9] ETSI TS 133 222: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (3GPP TS 33.222)".
- [10] ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220)".
- [11] 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".
- [12] ETSI TS 183 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; User-Network Interface Protocol Definitions".
- [13] 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".
- [14] 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".
- [15] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".
- [16] 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)".
- [17] ISO/IEC 11770-1 (2010): "Information technology - Security techniques - Key management - Part 1: Framework".
- [18] ITU-T Recommendation X.811: "Information Technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework".
- [19] ITU-T Recommendation X.812: "Information Technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework".
- [20] ITU-T Recommendation X.814: "Information Technology - Open Systems Interconnection - Security frameworks for open systems: Confidentiality framework".
- [21] ITU-T Recommendation X.815: "Information Technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework".
- [22] 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".
- [23] IETF RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".
- [24] IEEE 802.1x: "Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control".
- [25] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".
- [26] ETSI TS 187 003 Release 1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".