

ETSI TS 187 001 V3.9.1 (2014-07)



TECHNICAL SPECIFICATION

**Network Technologies (NTECH);
NGN SECURITY (SEC);
Requirements**

Reference

RTS/NTECH-00008-SEC-REQ

Keywords

security, service

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>

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 only prevailing document is the print of the Portable Document Format (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 or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2014.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI 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
Modal verbs terminology.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definitions and abbreviations.....	7
3.1 Definitions.....	7
3.2 Abbreviations	8
4a Security Objectives.....	9
4 Security Requirements	12
4.1 Security Policy Requirements	12
4.2 Authentication, Authorization, Access Control and Accountability Requirements	12
4.3 Identity and Secure Registration Requirements	15
4.4 Communications and Data Security Requirements	15
4.4.1 General Communications and Data Security Requirements	15
4.4.2 Integrity and Replay Protection Requirements	16
4.4.3 Confidentiality Requirements	16
4.5 Privacy Requirements.....	17
4.6 Key Management Requirements	18
4.7 Secure Management Requirements	18
4.8 NAT/Firewall Interworking Requirements	18
4.9 Non-Repudiation Requirements	18
4.10 Availability and DoS protection Requirements.....	18
4.11 Assurance Requirements	19
4.12 Requirements on Strength of Security Mechanisms.....	19
4.13 IPTV Security Requirements.....	19
4.13.1 Common IPTV Security Requirements	19
4.13.2 IPTV Service Protection Requirements	20
4.13.3 IPTV Content Protection Requirements	20
4.13.4 IMS-based IPTV Security Requirements.....	20
4.13.5 Non-IMS-based IPTV Security Requirements.....	21
4.13.6 Availability and DoS Protection Requirements	21
4.14 DRM.....	21
4.15 Media Security Requirements	22
4.15.1 Common Media Security Requirements	22
4.15.1.1 Regulatory Requirements.....	22
4.15.1.2 Non-broadcast media paths	22
4.15.1.3 NGN Requirements.....	22
4.15.1.4 NGCN Requirements	23
4.15.2 IMS-based Media Security Requirements	23
4.15.3 Non-IMS-based Media Security Requirements	23
4.16 Security Requirements to Counter Unsolicited Communications	23
4.17 Business communication security requirements.....	23
4.17.1 General security requirements	23
4.17.2 Specific security requirements for NGN/NGCN interconnection.....	24
4.17.3 Specific security requirements for hosted enterprise services	24
4.17.4 Specific security requirements for business trunking application.....	24
4.17.4.1 Security requirements for (subscription-based) business trunking application.....	24
4.17.4.2 Security requirements for (peering-based) business trunking application.....	24

4.17.5	Specific security requirements for virtual leased line	24
4.18	NAT Traversal Security Requirements	24
4.19	Home Networking Security Requirements	25
4.19.1	Confidentiality requirements	25
4.19.2	Identification, authentication and authorization requirements	25
4.19.3	Integrity requirements	26
4.19.4	Availability and DoS protection requirements	26
4.19.5	Service protection and/or content protection software upgrade security requirements	26
4.20	H.248 Security Requirements	27
5	NGN Security Release 2 Requirements Mapping	28
5.1	Network Access SubSystem (NASS)	28
5.2	Resource and Admission Control Subsystem (RACS)	30
5.3	The Core IP Multimedia Subsystem (IMS)	31
5.4	The PSTN/ISDN Emulation subsystem (PES)	33
5.5	Application Server (AS)	34
Annex A (informative): Bibliography		36
Annex B: Void		37
Annex C (informative): Trust domains in NGN		38
C.1	Definition of trust for the NGN - analysis	38
C.2	Requirements for creation of trusted channel	39
C.2.1	Functional security requirements for trusted channel in the NGN	39
C.3	Existing NGN capabilities	39
Annex D (informative): Security Objective Categories		40
D.1	Security Objective Categories Definitions	40
Annex E (informative): Security Objectives		41
E.1	General objectives	41
E.2	Security objective category confidentiality	41
E.3	Security objective category integrity	42
E.4	Security objective category availability	42
E.5	Security objective category authenticity	42
Annex F (informative): Change history		43
History		44

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://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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Network Technologies (NTECH).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**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.

Introduction

The TISPAN NGN R3 security is defined by the security requirements in the present document, while the architectural aspects and stage 2 implementations outline are covered in the Security Architecture for R3 (TS 187 003 [1]).

1 Scope

The present document defines the security requirements pertaining to TISPAN NGN Release 3. The present document holds requirements for the various NGN subsystems defined at a stage 1 level. The present document covers security requirements for both the NGN core network, and the NGN access network(s).

The main scope of the security requirements for the different subsystems are to identify requirements in the following main areas:

- Security Policies.
- Authentication, Authorization, Access Control and Accountability.
- Identity and Secure Registration.
- Communications and Data Security Requirements (including confidentiality, integrity aspects).
- Privacy.
- Key Management.
- NAT/Firewall Interworking.
- Availability and DoS protection.
- Assurance.
- Strength of Security Mechanisms.

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 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".
- [2] 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)".
- [3] 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)".
- [4] ETSI EG 202 238: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Evaluation criteria for cryptographic algorithms".