

ETSI TS 187 001 V2.1.5 (2008-10)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECURITY (SEC); Requirements

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/e341d13e-81f7-4d86-af13-a1923ec0f8bd/etsi-ts-187-001-v2.1.5-2008-10>



Reference

RTS/TISPAN-07026-NGN-R2

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

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 2008.
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.

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	7
2.2 Informative references.....	7
3 Definitions and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations	8
4 Security Requirements	9
4.1 Security Policy Requirements	9
4.2 Authentication, Authorization, Access Control and Accountability Requirements	10
4.3 Identity and Secure Registration Requirements	12
4.4 Communications and Data Security Requirements	12
4.4.1 General Communications and Data Security Requirements	12
4.4.2 Integrity and Replay Protection Requirements	13
4.4.3 Confidentiality Requirements	14
4.5 Privacy Requirements.....	14
4.6 Key Management Requirements	15
4.7 Secure Management Requirements	15
4.8 NAT/Firewall Interworking Requirements	15
4.9 Non-Repudiation Requirements	15
4.10 Availability and DoS protection Requirements	15
4.11 Assurance Requirements	16
4.12 Requirements on Strength of Security Mechanisms.....	16
4.13 IPTV Security Requirements.....	16
4.13.1 Common IPTV Security Requirements	16
4.13.2 IPTV Service Protection Requirements	17
4.13.3 IPTV Content Protection Requirements	17
4.13.4 IMS-based IPTV Security Requirements.....	17
4.13.5 Non-IMS-based IPTV Security Requirements.....	17
4.13.6 Availability and DoS Protection Requirements	18
4.14 DRM.....	18
4.15 Media Security Requirements	18
4.15.1 Common Media Security Requirements.....	18
4.15.1.1 Regulatory Requirements.....	18
4.15.1.2 Non-broadcast media paths	19
4.15.1.3 NGN Requirements.....	19
4.15.1.4 NGCN Requirements	19
4.15.2 IMS-based Media Security Requirements	19
4.15.3 Non-IMS-based Media Security Requirements	20
4.16 Security Requirements to Counter Unsolicited Communications	20
4.17 Business communication security requirements.....	20
4.17.1 General security requirements	20
4.17.2 Specific security requirements for NGN/NGCN interconnection.....	20
4.17.3 Specific security requirements for hosted enterprise services	20
4.17.4 Specific security requirements for business trunking application.....	20
4.17.4.1 Security requirements for (subscription-based) business trunking application.....	20
4.17.4.2 Security requirements for (peering-based) business trunking application.....	20
4.17.5 Specific security requirements for virtual leased line	21
4.18 NAT Traversal Security Requirements	21
4.19 Home Networking Security Requirements.....	21

4.20	H.248 Security Requirements.....	22
5	NGN Security Release 2 Requirements Mapping.....	22
5.1	Network Access SubSystem (NASS).....	23
5.2	Resource and Admission Control Subsystem (RACS).....	24
5.3	The Core IP Multimedia Subsystem (IMS).....	25
5.4	The PSTN/ISDN Emulation subsystem (PES).....	28
5.5	Application Server (AS).....	28
Annex A (informative): Bibliography.....		30
Annex B (informative): H.248 Security.....		31
B.1	Background	31
B.2	Challenging the assumption	31
B.3	Possible disadvantages	32
Annex C (informative): Trust domains in NGN.....		33
C.1	Definition of trust for the NGN - analysis.....	33
C.2	Requirements for creation of trusted channel.....	34
C.2.1	Functional security requirements for trusted channel in the NGN	34
C.3	Existing NGN capabilities.....	34
History		35

iTeh STANDARD PREVIEW
 (standards.iteh.ai)
 Full standard:
<https://standards.iteh.ai/catalog/standards/sist/es-41d13e-8117-4d86-af3-a0923ec088bd/etsi-ts-187-001-v2.1.5-2008-10>
 10

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).

Introduction

The TISPAN NGN R1 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 R1 (TS 187 003 [1]).

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/e341d13e-8117-4d86-af13-a1923ec0f8bd/etsi-ts-187-001-v2.1.5-2008-10>
10

1 Scope

The present document defines the security requirements pertaining to TISPAN NGN Release 2. 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 requirement 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 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>.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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 187 003: "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".

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] ISO 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".
- [i.2] IEEE 802.1X: "Port Based Network Access Control".
- [i.3] ISO 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components".
- [i.4] IETF RFC 3324: "Short Term Requirements for Network Asserted Identity".
- [i.5] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".
- [i.6] ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); H.248 Profile for controlling Access and Residential Gateways".
- [i.7] ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Lawful interception functional entities, information flow and reference points".
- [i.8] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF) (3GPP TS 33.310)".
- [i.9] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)".
- [i.10] ISO 27000: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".
- [i.11] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".
- [i.12] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imangement and their resolution in the NGN".

- [i.13] 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 (3GPP TS 24.229)".

3 Definitions and abbreviations

3.1 Definitions

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

anonymous communication: anonymous communication session is given when a user receiving a communication session cannot identify the originating user

trusted channel: means by which an NGN and a remote NGN/NGCN can communicate with necessary confidence to support the security policies of the NGN (from ISO 15408-1 [i.1])

trusted path: means by which a user and a NGN/NGCN can communicate with necessary confidence to support the security policies of the NGN/NGCN (from ISO 15408-1 [i.1])

trusted domain: in the context of one or more NGNs interconnected by the NNI as defined in TS 124 229 [i.13] clause 4.4 then trust is achieved by implementing one or more of the security mechanisms defined in TS 187 003 [1]

3.2 Abbreviations

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

3G	3 rd Generation
3GPP	3 rd Generation Partnership Project
AA	Authentication & Authorization
ACR	Anonymous Communications Rejection
AF	Application Function
AGW	Access Gateway
ALG	Application Layer Gateway
AP	Authentication Proxy
AS	Application Server
CNG	Customer Network Gateway
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSCF	Call Session Control Function
DoS	Denial-of-Service
EAP-AKA	Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement
HSS	Home Subscriber Server
ID	IDentity
IKE	Internet Key Exchange
IMPU	IMS PUblic user ID
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISIM	IMS Subscriber Identity Module
IT	Information Technology
MAC	Message Authentication Code
MD	Message Digest
NAF	operator controlled Network Application Function
NASS	Network Access SubSystem
NAT	Network Address Translation
NDS	Network Domain Security
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
NICC	Network Interoperability Consultative Committee

PAI	Public Administration International
P-CSCF	Proxy - Call Session Control Function
PES	PSTN/ISDN Emulation Subsystem
RACS	Resource Admission Control Subsystem
RGW	Residential Gateway
S-CSCF	Serving - Call Session Control Function
SEGF	SEcurity Gateway Functions
SIP	Session Initiation Protocol
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TOE	Security Functions
TS	Technical Specification
TSF	Target of Evaluation
UAS	User Agent Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System

4 Security Requirements

Security requirements described in clause 4 are identified by a symbolic security requirement identifier (e.g. R-SP-n) for quick reference and along with some textual description. The security requirements are listed without any implied preference or priority. It is pointed out that not all security requirements are mutually exclusive, but there is indeed some unavoidable overlap among them.

High level Objectives

The NGN shall support a secure and trustworthy environment for customers, network operators and service providers to meet a set of comprehensive and fundamental security requirements.

Given the service requirements, the security objectives are to prevent masquerade, DoS, manipulation of data, fraud and misuse of the network, abuse of one type of network through interconnection from a less secure environment.

ISIM shall be hosted on a UICC. Use of the ISIM on UICC is the preferred solution for achieving the security requirements to access the NGN IMS features. This does not preclude existing solutions such as e.g. Digest Authentication to allow early legacy implementations. The ISIM may reside within the device itself, or be accessed remotely, via a local interface to the "device holding the UICC".

Security requirements for users, service providers (access, application) may vary. The NGN security architecture shall not be limited to a single security policy. Each of the security services (authentication, data integrity, replay detection, confidentiality, etc.) must have the capability to be used independently of the others, as far as possible. The selection of services should be based on policy.

Security mechanisms needs to provide capabilities to allow for extensibility for new security mechanism and protocols.

Security mechanisms should not introduce new DoS attacks. Some security mechanisms and algorithms require substantial processing or storage, in which case the security protocols should protect themselves as much as possible against flooding attacks that overwhelm an endpoint with such processing or storage. Satisfying the requirement for high availability implies being able to mitigate denial-of-service attacks.

4.1 Security Policy Requirements

A security policy defines the legitimate users of a system and what they are allowed to do. It states what information must be protected from which threats. In environments with heterogeneous user communities, multiple vendors' equipment, differing threat models, and uneven deployment of security functionality, assurance that security is functioning correctly is extremely difficult without enforceable policies.

- (R-SP- 1) The TISPAN NGN network shall be logically and physically divided into security domains allowing for separation of application (e.g. IMS) and transport (e.g. ADSL or UMTS). Also different operators of similar networks (e.g. IMS) shall be able to operate their own security policies.

- (R-SP- 2) Security mechanisms and other parameters beyond default security mechanisms shall be configurable. This shall be static for NNI interface and may be negotiated for UNI interfaces. The security mechanism negotiation shall have a certain minimum level to be defined by the security domain; e.g. avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.
- (R-SP- 3) The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.
- (R-SP- 4) The UE shall always offer encryption algorithms for P-CSCF to be used for the session and the P-CSCF policy shall define whether to use encryption or not.
- (R-SP- 5) The UE and the P CSCF shall negotiate the integrity algorithm that shall be used for the session.
- (R-SP- 6) The policy of the HN shall be used to decide if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles.
- (R-SP- 7) The security gateway functions (SEGF) shall be responsible for enforcing security policies for the interworking between networks.

NOTE: The actual inter-security domain policy is not standardized and is left to the discretion of the roaming agreements of the operators.

- (R-SP- 8) SEGFs are responsible for security sensitive operations and shall offer capabilities for secure storage of long-term keys used for IKE authentication.

4.2 Authentication, Authorization, Access Control and Accountability Requirements

General Access authentication

- (R-AA- 1) Access to NGN networks, services, and applications shall be provided for authorized users only.
- (R-AA- 2) NGN R1 and R2 IMS authentication shall support early deployment scenarios (with support for legacy equipments), although it is optional for operators to deploy such scenarios.
- (R-AA- 3) In non-early deployment scenarios, IMS authentication shall be independent from access authentication.
- (R-AA- 4) An ISIM shall be used to access any IMS service, however, exceptions may be allowed for emergency calls and early deployment scenarios.
- (R-AA- 5) ISIM based Authentication between the IMS-subscriber and the network shall comply to the authentication part of Access Security for IP-based services TS 133 203 [2].
- (R-AA- 6) ISIM based Re-authentication of an IMS-subscriber shall comply to the authentication part of Access Security for IP-based services TS 133 203 [2].
- (R-AA- 7) It shall be possible to prevent the use of a particular ISIM to access NGN networks and services and it should be possible to revoke a specific ISIM.
- (R-AA- 8) NGN relevant ISIM specific information shall be protected against unauthorized access or alteration.
- (R-AA- 9) User authentication may either be hardware-based (for 3GPP UE: ISIM; i.e. proof by possession of a physical token) or be software-based (i.e. proof by knowledge of some secret information).

Early Deployments

- (R-AA- 10) User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as an early deployment scenario.

(R-AA- 11) Where both Digest and ISIM solutions are deployed by an NGN IMS operator, that operator shall determine the authentication mechanism (SIP Digest or ISIM-based) on a per-user basis. The authentication mechanism shall be enforced according to both the subscription information in the user's service profile and the specific policies of the NGN IMS operator. Where a terminal supports the ISIM solution and the network operator supports both ISIM and early deployment solutions, ISIM solution shall be used.

(R-AA- 12) Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.

(R-AA- 13) For the special early deployment scenarios (see note 1), where IMS authentication is linked to access authentication, it shall be possible to gain access to IMS services after an authentication procedure. This authentication provides simultaneous access to the access network and IMS services.

NOTE 1: The two special early deployment scenarios are (also referred to as NASS Bundled authentication):

(A). IMS authentication is linked to access line authentication (no nomadicity).

(B). IMS authentication is linked to access authentication for IP Connectivity (limited nomadicity can be provided).

NOTE 2: Access authentication may result in IMS services being tied to the access point (line) or to the current IP Connectivity (device). In the latter case limited nomadicity may be available. No IMS specific authentication is therefore required from the CPE/Terminal to gain access to IMS services.

(R-AA- 14) The NGN subsystems shall be able to be able to define and enforce policy with respect to validity of user authorization.

Ut Interface

(R-AA- 15) Mutual authentication shall be supported between the UE and the AS before providing authorization.

(R-AA- 16) It should also be possible to support an Authentication Proxy based architecture.

NOTE 1: The purpose of the AP is to separate the authentication procedure and the AS specific application logic to different logical entities.

(R-AA- 17) Mutual authentication shall be supported between the UE and the AP.

(R-AA- 18) The AP shall decide whether a particular subscriber (i.e. the UE), is authorized to access a particular AS.

(R-AA- 19) If an AP is used, the AS shall only authorize the access request to the requested resource.

NOTE 2: The AS does not need to explicitly authenticate the user.

NASS

(R-AA- 20) Mutual authentication should be supported between the CPE and the NASS during access network level registration.

(R-AA- 21) The access network shall be able to authenticate and authorize the access subscriber.

(R-AA- 22) Authentication and authorization to the Access Network is controlled by the operator of the Access Network.

(R-AA- 23) The attributes required for authentication of a user by the access network maybe provided by the network operator to whom the user has a NGN IMS subscription.

(R-AA- 24) NASS shall support both the use explicit (e.g. PPP or IEEE 802.1x [i.2]) and/or implicit line authentication (e.g. MAC address authentication or line authentication) of the users/subscribers. In the case of the implicit access authentication, it shall rely only on an implicit authentication through physical or logic identity on the layer 2 (L2) transport layer.

(R-AA- 25) In case the CNG is a routing modem and the Customer Premises Network (CPN) is a private IP realm, authentication shall be initiated from the CNG.