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

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/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://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".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[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: " IEEE Standard for Local and metropolitan area networks 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] Void.

[i.7] Void.

[i.8] Void.

[i.9] Void.

[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 imanagement 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)".

[i.14] ISO/IEC TR 13335 (2004): "Information technology -- Guidelines for management of IT Security".

[i.15] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis".

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 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]

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])

3.2 Abbreviations

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

3G	3rd Generation
3GPP	3rd 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
CND	Customer Network Device
CNG	Customer Network Gateway
CP	Content Protection
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSCF	Call Session Control Function
CSP	Content Service Provider
DoS	Denial-of-Service
DRM	Digital Right Management
HSS	Home Subscriber Server
HW/SW	Hardware/Software
ID	IDentity
IKE	Internet Key Exchange
IMPU	IMS Public user ID
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol based Television
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
NNI	Network to Network Interface
PAI	Public Administration International
P-CSCF	Proxy - Call Session Control Function
PES	PSTN/ISDN Emulation Subsystem
RACS	Resource Admission Control Subsystem
RTP	Realtime Transport Protocol
RTSP	Real Time Streaming Protocol
S-CSCF	Serving - Call Session Control Function
SEGF	Security Gateway Functions
SIP	Session Initiation Protocol
SP	Security Policy Requirements
SP/CP	Service Protection/Content Protection
SPDF	Service Policy Decision Function
TCP	Transport Control Protocol
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking

TLS Transaction Layer Security
TS Technical Specification
TSF Target of Evaluation
TVRA Threat Vulnerability Risk Analysis
UAS User Agent Server
UE User Equipment
UICC Universal Integrated Circuit Card
UMTS Universal Mobile Telecommunication System
UNI User to Network Interface

4a Security Objectives

Whilst the primary objective of the NGN is to provide a secure and trusted framework for users a complete list of objectives is given in table 1a.

The domain to which an objective applies is one of the following:

- System, e.g. Architecture, Policy, NGN, NASS, RACS
- Service, e.g. IPTV, VoIP
- Technology, e.g. NAT Traversal, SIP, DIAMETER.

Table 1a: NGN security objectives (multi-page table)

Objective identifier	Objective text	Domain	Functional requirement identifier
OBJ-1	The NGN should be logically and physically divided into security domains allowing for separation of application, transport and content in accordance with the Framework Directive.	System - Architecture	R-SP- 1
OBJ-2	NGN operators should be able to operate their own security policies.	System - Policy	R-SP- 1
OBJ-3	Security mechanisms and other parameters beyond default security mechanisms should be statically configured at the NNI.	System - management and configuration	R-SP- 2
OBJ-4	Security mechanisms and other parameters beyond default security mechanisms should be configurable dynamically at the UNI.	System - management and configuration	R-SP- 2
OBJ-5	Users should be able to reject communications that do not conform to their minimum security policy.	System - Policy	R-SP- 2
OBJ-6	Security mechanisms should be partitioned such that each of the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other.	System - Architecture	R-SP- 3
OBJ-7	NGN operators may deploy alternatives to the IMS authentication defined in TS 133 203 [2] in early deployment.	Service - Authentication	R-AA- 2
OBJ-8	In the NGN authentication in one security domain should be independent of authentication in any other security domain.	Service - Authentication	R-AA- 3
OBJ-9	NGN operators should be able to prevent the use of a particular ISIM to access NGN networks and services.	Technology - ISIM	R-AA- 7
OBJ-10	NGN operators should be able to revoke a specific ISIM.		R-AA- 7
OBJ-11	NGN relevant ISIM specific information should be protected against unauthorized access.	Technology - ISIM	R-AA- 8
OBJ-12	NGN relevant ISIM specific information should be protected against unauthorized alteration.	Technology - ISIM	R-AA- 8
OBJ-13	Where passwords are used for authentication they should be protected from exposure during transmission.	Service - Authentication	R-AA- 12
OBJ-14	Each NGN security domain should have and enforce a user authorization policy.	Service - Authentication	R-AA- 14
OBJ-15	An NGN security domain should be able to act as a proxy for another peer domain with respect to authentication.	System - Architecture	R-AA- 16

Objective identifier	Objective text	Domain	Functional requirement identifier
OBJ-16	An NGN security domain acting as a proxy for another peer domain should follow its own policy with respect to routing of authorization requests.	System - Architecture	R-AA- 18
OBJ-17	Mutual authentication should be supported between the CPE and the NASS during access network level registration.	Service - Authentication	R-AA- 20
OBJ-18	Data held on the ISIM should be updated by authorized parties only.	Technology - ISIM	R-CD- 9
OBJ-19	The NGN should provide means to protect sensitive data (such as Presence information and notifications) from attack (e.g. eavesdropping, tampering, and replay attacks).	System	R-CD- 10
OBJ-20	The NGN should provide mechanisms to ensure the origin, integrity and freshness of authentication data.	Service - Authentication	R-CD- 14
OBJ-21	Confidentiality of signalling and control messages should be managed by the security policy of the security domain.	System - Policy	R-CD- 19
OBJ-22	The security policy should associate each security association with specific functions (e.g. confidentiality, integrity) and identify the algorithms to be used.	System - Policy	R-CD- 19
OBJ-23	The NGN should ensure that user-related data that is stored or processed by a provider are visible only to authorized parties.		R-CD- 22
OBJ-24	Each domain of the NGN should ensure that details of the network topology of the domain are visible only to authorized parties.		R-P- 1
OBJ-25	The NGN should ensure that user location and usage patterns are visible only to authorized parties.		R-P- 2
OBJ-26	The NGN should ensure that user identity data is visible only to authorized parties.		R-P- 3
OBJ-27	The NGN should provide mechanisms to prove the authenticity of a user identity presented for an incoming call to a user where the call is wholly within that operator's network (i.e. originating and terminating parties are subscribers to, and resident in, a single NGN).		R-P- 7
OBJ-28	The NGN should ensure that presence services respect the privacy policies of the affected parties.		R-P- 9
OBJ-29	The NGN should provide a means for an affected user to manage their privacy policy per call or per session.		R-P- 9
OBJ-30	The NGN should ensure that presence services respect the privacy policies of the affected parties.		R-P- 10
OBJ-31	The NGN should ensure that presence services respect the privacy policies of the affected parties.		R-P- 11
OBJ-32	The NGN should provide a means for an affected user to manage their privacy policy per call or per session.		R-P- 12
OBJ-33	Each domain of the NGN should ensure that details of the network topology of the domain are visible only to authorized parties.		R-P- 14
OBJ-34	The NGN should provide means to detect denial-of-service attacks.		
OBJ-35	The NGN should provide means to mitigate denial-of-service attacks.		R-AD- 3
OBJ-36	Availability of EMTEL PSAPs should be maintained when the system is subjected to DoS attacks.		R-AD- 5
OBJ-37	The security association between an NGN IPTV service user and the NGN IPTV service provider should define mechanisms to assure the integrity and confidentiality of communication and the authenticity of the user and provider.		R-IPTV-CN-3
OBJ-38	The NGN IPTV service protection functions applied on a service providing access to IPTV content should interoperate with Content Protection solutions.		R-IPTV-CN-7
OBJ-39	The NGN IPTV service and content protection functions should provide the means for retrieving related rights and/or keys for chosen protected content items.		R-IPTV-CP-6
OBJ-40	The NGN IPTV service should provide a means to prevent unauthorized use of content.		R-IPTV-CP-7
OBJ-41	The NGN IPTV service should provide a means to prevent unauthorized distribution of content.		R-IPTV-CP-8
OBJ-42	The NGN IPTV content protection functions should provide a means to prevent consumption of content after a specific time.		R-IPTV-CP-9

Objective identifier	Objective text	Domain	Functional requirement identifier
OBJ-43	The NGN IPTV service should provide a general framework for the integration of content protection solutions (e.g. DRM).		R-IPTV-DRM-1
OBJ-44	The NGN should support the integration of one or more DRM solutions for IPTV content protection.		R-IPTV-DRM-2
OBJ-45	An NGN operator should provide mechanisms to ensure the interception and handover of signalling of specific NGN users if required to by a lawful authority.		R-MS-REG-4
OBJ-46	An NGN operator should provide mechanisms to ensure the interception and handover of the content of communication of specific NGN users if required to by a lawful authority.		R-MS-REG-1
OBJ-47	An NGN operator should provide mechanisms to ensure the retention and handover of signalling of specific NGN users if required to by a lawful authority.		R-MS-REG-2
OBJ-48	An NGN should ensure that non-broadcast media paths are constructed such that eavesdropping cannot be achieved without intrusion to the media path.		R-MS-GEN-1
OBJ-49	An NGN should ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content.		R-MS-GEN-2
OBJ-50	An NGN should ensure that the key used for encryption is only known to the parties directly involved in the transfer of media over the broadcast path.		R-MS-GEN-3
OBJ-51	The NGN should ensure source and destination address authentication, confidentiality and integrity protection of media transfer in point-to-point topologies.		R-MS-3
OBJ-52	The NGN should ensure source and destination address authentication, confidentiality and integrity protection of media transfer in point-to-multipoint topologies.		R-MS-4
OBJ-53	The NGN should ensure source and destination address authentication, confidentiality and integrity protection of media transfer in broadcast topologies.		R-MS-5
OBJ-54	The NGN should provide the ability for an affected user to request the rating of an UC call.		R-UC-3
OBJ-55	The NGN should provide the ability for an affected user to challenge the ratings made by the UC detection system.		R-UC-4
OBJ-56	The NGN should provide the ability to the affected CSP to extract from the call signalling sufficient information to provide a UC rating for the call.		R-UC-5
OBJ-57	The NGN should provide a mechanism to convey the UC rating in the call signalling.		R-UC-6
OBJ-58	The NGN should provide a mechanism to allow variation in the call handling for calls with particular UC ratings.		R-UC-7
OBJ-59	NAT traversal in the NGN should minimize the number of messages that are transmitted solely for NAT traversal.		R-NAT TRAV-10
OBJ-60	NAT traversal in the NGN should minimize additional session setup delay.		R-NAT TRAV-12
OBJ-61	NAT traversal in the NGN should take into account the scalability, complexity and compatibility with other relevant NGN requirements.		R-NAT TRAV-15
OBJ-62	Any solution recommended for NAT traversal in the NGN should not impact the inherent ability of TLS to operate across NAT.		R-NAT TRAV-16
OBJ-63	Internally to the CPN, a CNG receiving private or other critical information (i.e. from a CND) should verify that the data was protected from unauthorized disclosure.		R-CPN-CR-3
OBJ-64	The authentication protocol in the CPN should be designed to cater for authentication failure.		R-CPN-IAAR-2
OBJ-65	On detection of any system failure or discontinuity not specifically handled by other mechanisms the CNG should revert to a known safe state.		R-CPN-AR-3

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.

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. The ISIM may reside within the device itself, or be accessed remotely, via a local interface to the "device holding the UICC".

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 needs 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 IMS authentication shall support early deployment scenarios, although it is optional for operators to deploy such scenarios.