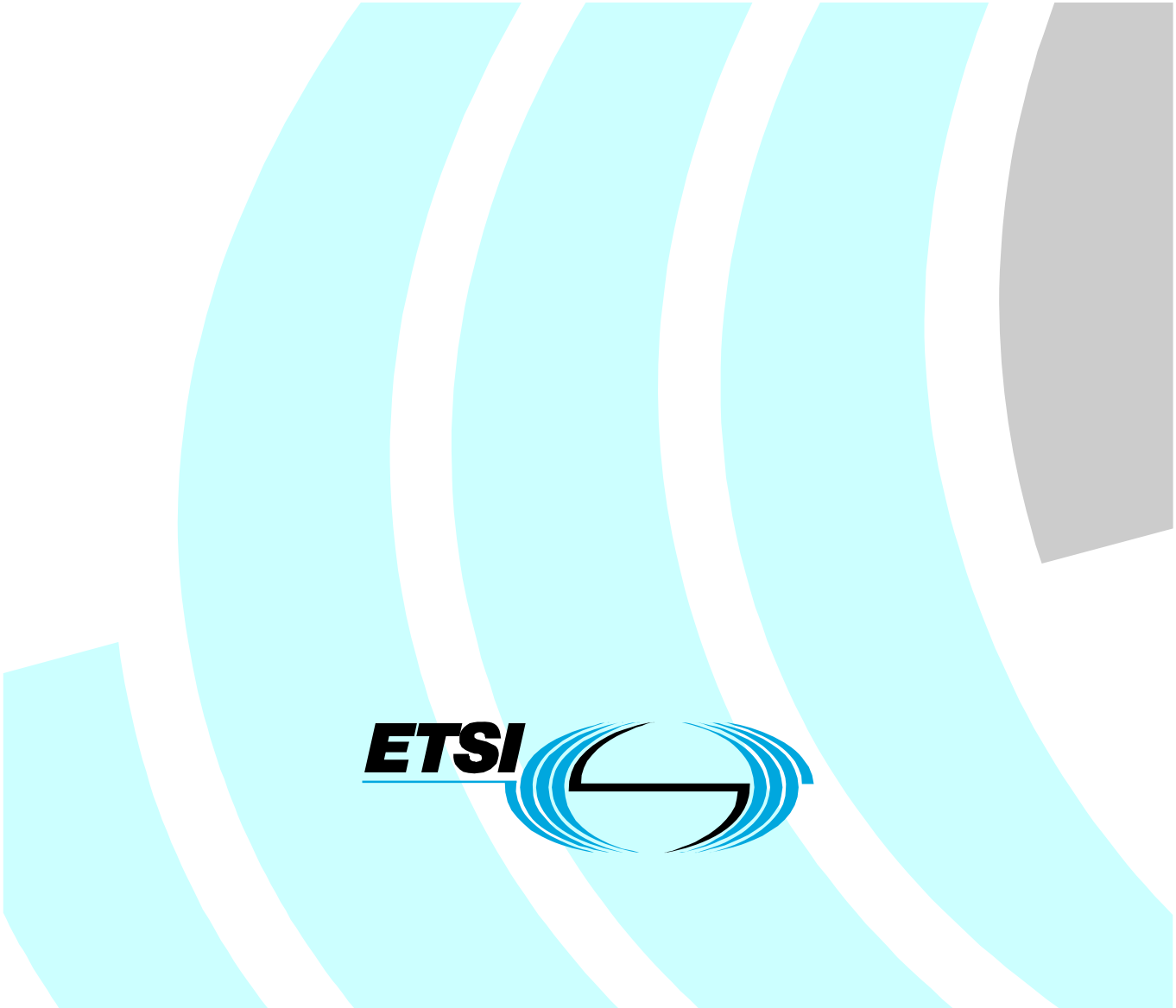
ETSI TS 187 001 V3.7.1 (2011-03)

Technical Specification

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



Reference
RTS/TISPAN-07036-NGN-R3

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

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).

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 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 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); LTE; 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); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

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: "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] ISO 27000: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

[i.7] 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.8] 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.9] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[i.10] ISO/IEC TR 13335:2004: "Information technology - Guidelines for management of IT Security".

[i.11] 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".

[i.12] ETSI EG 202 238: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Evaluation criteria for cryptographic algorithms".

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.9], 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
ADSL	Asymetrical Digital Subscriber Line
AF	Application Function
ALG	Application Layer Gateway
AP	Authentication Proxy
AS	Application Server
CND	Customer Network Gateway
CNG	Customer Network Gateway
CP	Content Protection
CPE	Customer Premises Equipment
CPF	Content Protection Function
CPN	Customer Premise Network
CPN	Customer Premises Network
CSCF	Call Session Control Function
CSP	Content Service Provider
DoS	Denial-of-Service
DRM	Digital Right Management
EMTEL	EMergency TELecommunications
HSS	Home Subscriber Server
HW	HardWare
ID	Identity
IKE	Internet Key Exchange
IMPU	IMS Public user ID
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol TeleVision
ISDN	Integrated Services Digital Network
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
NATP	Network Address and Port Translation
NDS	Network Domain Security
NGCN	Next Generation Corporate Network
NGN	Next Generation Network
NGN	Next Generation Network
NNI	Network to Network Interface
OIR	Originating Identification Restriction
PAI	Public Administration International
P-CSCF	Proxy - Call Session Control Function
PES	PSTN/ISDN Emulation Subsystem
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
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	Service Protection
SPF	Service Protection Function

SW	SoftWare
TCP	Transmission Control Protocol
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TS	Technical Specification
TSF	Target of Evaluation
TSP TOE	(Target of Evaluation) Security Policy
TVRA	Threat, Vulnerability and Risk Analysis
UA	User Agent
UAS	User Agent Server
UC	Unsolicited Communications
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UNI	User to Network Interface
VoIP	Voice over Internet Protocol

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

Objective identifier	Objective text	Domain	Functional requirement identifier
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
OBJ-16	An NGN security domain acting as a proxy for another peer domain should follow its own policy with respect to routing of authorisation 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 authorised 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 authorised 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 authorised parties.		R-P- 1
OBJ-25	The NGN should ensure that user location and usage patterns are visible only to authorised parties.		R-P- 2
OBJ-26	The NGN should ensure that user identity data is visible only to authorised 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 authorised 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

Objective identifier	Objective text	Domain	Functional requirement identifier
OBJ-40	The NGN IPTV service should provide a means to prevent unauthorised use of content.		R-IPTV-CP-7
OBJ-41	The NGN IPTV service should provide a means to prevent unauthorised 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
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 unauthorised 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 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 IMS authentication shall support early deployment scenarios, 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 on UICC; 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 more than one authentication mechanism are deployed by an NGN IMS operator, that operator shall determine the authentication mechanism (e.g. SIP Digest or ISIM-based) on a per-device 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.

(R-AA- 26) In case the CNG is a bridge, each UE shall authenticate with the NASS as the IP realm in the CPN is known to the Access Network.

RACS

(R-AA- 27) RACS and AF shall be mutually authenticated prior to resource authorization.

(R-AA- 27A) AF and SPDF in RACS shall be able to mutually identify each other when performing the authentication.

CPN - RACS

(R-AA- 28) RACS and CPN shall be mutually authenticated prior to resource authorization.

NOTE: For emergency services alternative procedures are required.

Other Specific Requirements

(R-AA- 28.1) A media gateway controller must be able to handle authentication of multiple media gateways, i.e. to maintain multiple security associations with different media gateways.

(R-AA- 28.2) Authentication of NGN users and authentication of NGN terminals shall be separate.

(R-AA- 29) Caller id and location information shall be stored according to the Common European regulatory framework by the EMTEL Service Provider. Caller ID and location information shall be validated by the EMTEL Service Provider.

4.3 Identity and Secure Registration Requirements

The following requirements aim to mitigate against masquerading, spoofing, and impersonation of NGN terminals, devices/systems (HW/SW) and users. The requirements aim to provide measures against identity theft, misuse/authorized use of NGN services/applications.

(R-IR- 1) It shall be possible to implicitly register IMPU(s). The implicitly registered IMPU(s) all belong to the same Service Profile. All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).

(R-IR- 2) An access identity shall be used for access authentication. This identity may or may not be used for other purposes.

(R-IR- 3) The line ID shall be possible to use for line authentication.

4.4 Communications and Data Security Requirements

Clause 4.4 contains such requirements that address communications and data security. Data, in this context, can mean either user data (e.g. voice, video, text stream) or management data.

4.4.1 General Communications and Data Security Requirements

General

(R-CD- 1) Confidentiality and integrity of IMS signalling shall be applied in a hop-to-hop fashion. (UE-to-P-CSCF and among other Nes).

NDS

(R-CD- 2) Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [3].

(R-CD- 3) All NDS/IP traffic shall pass through a SEGF (Security Gateway Function) before entering or leaving the security domain. IMS operators shall operate NDS/IP Za interface between SEGFs according to TS 133 210 [3].

(R-CD- 4) Security shall be provided within the network domain for the Cx interface.

Access Security

(R-CD- 5) An ISIM based solution for IMS access security (authentication, confidentiality and integrity protection) of signalling to and from the user, shall be supported.

(R-CD- 6) Secure link shall be provided between UE and the P-CSCF for protection of the Gm reference point.

(R-CD- 7) In case access authentication is independent from IMS authentication.

- Solutions for access to the NGN core shall provide for secure transfer of signalling to the NGN core independent of the access technology.
- Solutions for access to the NGN core shall provide for secure transfer of signalling to the NGN core independent of the presence of intermediate IP networks connecting the NGN access with the NGN core.
- Solutions for access to the NGN core shall allow for mutual authentication of end user and NGN core. It shall be possible for the terminal to authenticate the user.

(R-CD- 8) In the case where IMS authentication is linked to access line authentication the underlying access technology shall provide protection of NGN signalling and user data.

(R-CD- 9) ISIM specific information shall be updated in a secure manner.

Ut

(R-CD- 10) It shall be possible to protect sensitive data (such as Presence information and notifications) from attacks (e.g. eavesdropping, tampering, and replay attacks).

RACS

(R-CD- 11) Void.

Other Specific Requirements

(R-CD- 12) All data related to configuring the UE through the e3 reference point shall be protected against loss of confidentiality and against loss of integrity.

4.4.2 Integrity and Replay Protection Requirements

General

(R-CD- 13) Integrity protection of signalling, control communications and of stored data shall be provided.

(R-CD- 14) It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key.

Access Security

(R-CD- 15) Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling.

NDS

(R-CD- 16) Integrity protection between Network Elements (e.g. between CSCFs, and between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [3].

Ut

(R-CD- 17) Data integrity shall be supported between the UE and the Application Server.

RACS

(R-CD- 17.1) RACS shall ensure integrity of all information exchanged over the e4 reference point.

RACS - CPN

(R-CD- 17.2) RACS shall ensure integrity of all policy related resource information exchanged between CPN and RACS.

NOTE: This requires that RACS is the validator of the integrity of the data exchanged, and that CPN is the generator of the integrity check data.

4.4.3 Confidentiality Requirements

General

(R-CD- 18) Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.

(R-CD- 19) Confidentiality of signalling and control messages shall be enforced if required by the application or in environments where the security policy demands confidentiality. The mechanism should allow a choice in the algorithm to be used.

Access Security

(R-CD- 20) IMS specific confidentiality protection shall be provided for the SIP signalling between UE and P-CSCF.

(R-CD- 20.1) There shall be means to enable confidentiality protection on all communication over interface e5.

(R-CD- 20.2) There shall be means to enable confidentiality protection of all information exchanged over interface e2.

NDS

(R-CD- 21) Confidentiality protection between Network Functions (e.g. between CSCFs, or between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [3].

Other Specific Requirements

(R-CD- 22) It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.

CPN - RACS

(R-CD- 23) RACS shall ensure confidentiality of all policy related resource information exchanged between CPN and RACS.

4.5 Privacy Requirements

(R-P- 1) It shall be possible to protect the network topology from exposure toward other domains. It shall also be possible for a security domains to define and implement protection against traffic analysis for signalling and management protocols.

(R-P- 2) User location and usage patterns shall be kept from unwanted disclosure.

(R-P- 3) It shall be possible to protect the confidentiality of user identity data.

(R-P- 4) Anonymous communication sessions shall be supported in NGN either in a permanent mode or in a temporary mode communication by call. In this case the originating party identity shall not be presented to the destination party. The network to which the destination party is connected to is responsible to handle this service.

(R-P- 5) NGN shall support the specific case where the destination party has an override right (e.g. emergency communication sessions), and the originating party identity is provided to the destination party independent whether or not this communication session is anonymous.

(R-P- 6) The Anonymous Communications Rejection (ACR) simulation service shall allow the served user to reject incoming communication from users or subscribers who have restricted the presentation of their originating identity according to the OIR simulation service.

(R-P- 7) The NGN shall support mechanisms for the network operator to guarantee 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- 8) The NGN shall provide mechanisms that allow to present the identity of the session originator, if this is not restricted by the session originator.

(R-P- 9) The privacy aspect of presence information and the need for authorization before providing presence information shall be configurable by the user (i.e. presentity).

(R-P- 10) A principal of a presentity shall, at any time, be able to control to whom, for how long and what (all or part of) presence information of the presentity is provided, and a principal of a watcher shall, at any time, be able to control to whom, for how long and what (all or part of) watcher information of the watcher is provided.

(R-P- 11) Any services using the presence information shall ensure privacy agreement before releasing presence information. The presence service does not address deployment specific issues (e.g. where agreements are stored or how they are negotiated). It only gives requirements for privacy management.

(R-P- 12) It shall be possible for the sender of the message to request to hide its public ID from the recipient.

(R-P- 13) Users may select the Identity presented when starting a session or sending a message. It shall be possible to verify this identity and to initiate a session or message in reply.

(R-P- 14) It shall be possible to protect the CPN topology from exposure toward the NGN.

(R-P- 15) The CPN transmitting information to the RACS shall not disclose CPN internal (private or other critical) information to the RACS.

4.6 Key Management Requirements

(R-KM- 1) Key management and key distribution between SEGFs shall comply to the Network Domain Security TS 133 210 [3].

(R-KM- 2) The UE and the AS shall be able to resume a previously established secure session.

(R-KM- 3) The key management mechanism must be able to traverse a NAT/NATP device.

4.7 Secure Management Requirements

NOTE: Security Management requirements are for further study.

4.8 NAT/Firewall Interworking Requirements

Firewall is here understood in a generic sense. A firewall could be an Application-Level Gateway (ALG), a proxy, a packet-filter, a NAT/NATP device or a combination of all of those. A Security Gateway Function is an entity on the border of the IP security domain and is used to secure native IP based protocols over the Za interfaces.

(R-NF- 1) NGN security protocols shall work with commonly-used firewalls and shall work in environments with NAT/NATP.

(R-NF- 2) Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.

(R-NF- 3) The SEGFs may include filtering policies and firewall functionality not required in TS 133 210 [3].

4.9 Non-Repudiation Requirements

NOTE: Non-repudiation requirements are for further study.

4.10 Availability and DoS protection Requirements

(R-AD- 1) Mechanisms shall be provided to mitigate denial-of-service attacks.

(R-AD- 2) Provide access control mechanisms to ensure that authorized users only can access the service.

(R-AD- 3) It shall be possible to prevent intruders from restricting the availability of services by logical means.

(R-AD- 4) Availability of and accuracy of location information shall be provided for the EMTEL services.

(R-AD- 5) Availability of EMTEL PSAPs shall not be decreased by DoS attacks. EMTEL PSAPs shall be able to reconnect.

4.11 Assurance Requirements

(R-AS- 1) The TISPAN NGN shall provide guidance for evaluating and certifying NGN equipment and systems.

(R-AS- 2) Security implications of potential misuse of protocols used in NGN shall be documented through a TVRA. This enables users to assess the security they need before deploying the given protocol.

4.12 Requirements on Strength of Security Mechanisms

The guidelines defined in EG 202 238 [i.12] shall be followed when defining or selecting cryptographic algorithms in TISPAN.

4.13 IPTV Security Requirements

4.13.1 Common IPTV Security Requirements

NOTE: When delivering the security information (e.g. the licenses or keys) to the subscribers (especially large amount of subscribers), the impact to system performance should be taken into account.

(R-IPTV-C-1) The NGN IPTV service shall allow several kinds of users, named groups of users, entities acting on behalf of users and entities acting on behalf of named groups of users.

(R-IPTV-C-2) The NGN IPTV service shall assign unique and non-forgeable user identities to users.

(R-IPTV-C-3) The NGN IPTV service shall allow several (number to be decided) users to be associated with one subscription.

(R-IPTV-C-4) The NGN IPTV service shall uniquely authenticate all users to the IPTV service using unique and non-forgeable authentication credentials on a subscription basis.

(R-IPTV-C-5) The NGN IPTV service shall uniquely authorize all users to the IPTV service on a subscription basis.

(R-IPTV-C-6) The NGN IPTV service shall assign unique and non-forgeable identities to all subscribers and named groups of subscribers.

(R-IPTV-C-7) The NGN IPTV service shall uniquely authenticate all subscribers and named groups of subscribers to the IPTV service using unique authentication credentials.

(R-IPTV-C-8) The NGN IPTV service shall uniquely authorize all subscribers and named groups of subscribers to the IPTV service.

(R-IPTV-C-9) The NGN IPTV service shall assign unique and non-forgeable identities to all user devices.

(R-IPTV-C-10) The NGN IPTV service shall uniquely authorize all devices to the IPTV service.

(R-IPTV-C-11) The NGN IPTV service shall assign unique and non-forgeable identities to all IPTV sessions that are verifiable to users and devices.

(R-IPTV-C-12) The NGN IPTV service shall assign unique and non-forgeable identities to all IPTV service providers that are verifiable to users.

(R-IPTV-C-13) The NGN IPTV service shall provide a mechanism to authenticate and authorize the RTSP control messages from users.

(R-IPTV-C-14) The NGN IPTV service shall assign unique and non-forgeable identities to all IPTV content that are verifiable for users.

4.13.2 IPTV Service Protection Requirements

(R-IPTV-CN-1) The NGN IPTV service protection functions shall support distribution of access keys coming from the network according to the corresponding rights.

(R-IPTV-CN-2) The NGN IPTV service protection functions shall support means to protect the service-associated keys against unauthorized access, and ensure their integrity and confidentiality.

(R-IPTV-CN-3) The NGN IPTV service protection functions shall be able to authenticate and ensure the integrity and confidentiality of communication between the service and the user.

(R-IPTV-CN-4) The NGN IPTV service protection functions shall provide a means for protecting time-restricted services (e.g. subscription and pay-per-view).

(R-IPTV-CN-5) The NGN IPTV service protection functions shall provide an open framework allowing the operator to choose one or more protection solution.

(R-IPTV-CN-6) The NGN IPTV service protection functions applied on a service providing access to IPTV content shall not make any constraint on the way the content is protected.

(R-IPTV-CN-7) The NGN IPTV service protection functions applied on a service providing access to IPTV content should interoperate with Content Protection solutions.

4.13.3 IPTV Content Protection Requirements

(R-IPTV-CP-1) The NGN IPTV content protection shall authenticate and authorize the origin of all IPTV content to the receiving users.

(R-IPTV-CP-2) The NGN IPTV content protection shall verify the authenticity of the origin of all IPTV content to the receiving users.

(R-IPTV-CP-3) The NGN IPTV content protection shall provide end-to-end content confidentiality protection within regulatory constrains.

(R-IPTV-CP-4) The NGN IPTV service should provide end-to-end content integrity protection for an IPTV session.

(R-IPTV-CP-5) The NGN IPTV service shall control and restrict content on a content metadata basis for users.

(R-IPTV-CP-6) The NGN IPTV service and content protection functions shall provide the means for retrieving related rights and/or keys for chosen protected content items.

(R-IPTV-CP-7) The NGN IPTV service shall have a measure to restrict unauthorized usage of content (viewing, re-viewing, copying, etc.) for users.

(R-IPTV-CP-8) The NGN IPTV service shall have a measure to restrict unauthorized distribution of content for users.

(R-IPTV-CP-9) The NGN IPTV content protection functions shall provide a means for protecting time-restricted content usage.

(R-IPTV-CP-10) The NGN IPTV content protection functions shall provide an open framework allowing the operator to choose one or more protection solution.

4.13.4 IMS-based IPTV Security Requirements

NOTE: Reusing the existing IMS security mechanisms as much as possible should be taken into account.

4.13.5 Non-IMS-based IPTV Security Requirements

(R-IPTV-NIMS-1) The NGN IPTV service shall for each IPTV session uniquely link devices, users, named groups of users, entities acting on behalf of users to an IPTV session.

(R-IPTV-NIMS-2) The NGN IPTV service shall for each combined IPTV session uniquely link devices, users to an IPTV session.

(R-IPTV-NIMS-3) The NGN IPTV service shall assign unique identities to critical IPTV service logics on the devices that are verifiable for users.

(R-IPTV-NIMS-4) The NGN IPTV service shall assign non-forgeable identities to critical IPTV service logics on the devices that are verifiable for users.

(R-IPTV-NIMS-5) The NGN IPTV service shall authenticate and authorize critical IPTV service logics on the devices to the receiving user.

(R-IPTV-NIMS-6) The NGN IPTV service shall verify the authenticity of critical IPTV service logics on the devices to the receiving users.

(R-IPTV-NIMS-7) Refinement of DSF9: The NGN IPTV service shall uniquely authenticate all subscribers and named groups of subscribers when accessing private or sensitive information using unique authentication credentials.

(R-IPTV-NIMS-8) Refinement of DSF10: The NGN IPTV service shall uniquely authorize all subscribers and named groups of subscribers when accessing private or sensitive information.

(R-IPTV-NIMS-9) The NGN IPTV service shall provide end-to-end encryption of private or sensitive information on an IPTV session basis.

4.13.6 Availability and DoS Protection Requirements

(R-IPTV-AD-1) The NGN IPTV service shall be accessible to the authorized users, subscribers and devices according to the requirements of the IPTV service regarding timeliness and quality.

(R-IPTV-AD-2) The NGN IPTV service shall have measures to prevent DoS attacks posed upon the IPTV service to ensure fulfilment of the requirements of the IPTV service regarding timeliness and quality.

(R-IPTV-AD-3) The NGN IPTV service shall have measures to detect and act upon all DoS attacks posed upon the IPTV service (note that act might mean inform e.g. the system administrator of the event) to ensure fulfilment of the requirements of the IPTV service regarding timeliness and quality.

4.14 DRM

(R-IPTV-DRM-1) The NGN IPTV service shall provide a general framework open to the integration of content protection solutions (e.g. DRM).

(R-IPTV-DRM-2) One or more open fully standardized DRM solutions shall be supported with NGN IPTV content protection, including e.g. the key management, the delivery, and encryption and decryption operations of keys and content, and interfaces. All solutions shall be fully specified, permitting well-defined variations in operational behaviour without introducing proprietary elements to any part of the system. All such solutions shall have the same priority.

(R-IPTV-DRM-3) The fully standardized DRM solution shall fulfil the requirements as stated in clause 4.13.3 "IPTV Content Protection Requirements".

4.15 Media Security Requirements

4.15.1 Common Media Security Requirements

4.15.1.1 Regulatory Requirements

(R-MS-REG-1) An NGN shall provide mechanisms to prevent eavesdropping of traffic.

(R-MS-REG-2) An NGN shall provide mechanisms to prevent unauthorized recording and storage of traffic.

(R-MS-REG-3) An NGN shall provide mechanisms to prevent unauthorized interception of traffic.

(R-MS-REG-4) 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.

NOTE 1: This requirement is not strictly related to media but may be correlated to media provision.

(R-MS-REG-5) 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-6) 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.

NOTE 2: This requirement is not strictly related to media but may be correlated to media provision.

4.15.1.2 Non-broadcast media paths

(R-MS-GEN-1) 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-2) An NGN should ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content.

(R-MS-GEN-3) 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.

4.15.1.3 NGN Requirements

(R-MS-1) The NGN shall not provide support for end-to-end media security.

(R-MS-2) The NGN shall provide support for user-to-network media security (for the following security services Confidentiality, Integrity, Authenticity of source and destination end-points).

(R-MS-3) The NGN shall provide support for secure media transfer in point-to-point topologies.

(R-MS-4) The NGN shall provide support for secure media transfer in point-to-multipoint topologies.

(R-MS-5) The NGN shall provide support for secure media transfer in broadcast topologies.

(R-MS-6) An NGN shall provide mechanisms to prevent eavesdropping of traffic.

(R-MS-7) An NGN shall provide mechanisms to prevent unauthorized recording and storage of traffic.

(R-MS-8) An NGN shall provide mechanisms to prevent unauthorized interception of traffic.

(R-MS-9) 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-10) An NGN should ensure that broadcast media paths (e.g. radio) should be protected by encryption of media content.

(R-MS-11) 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.

4.15.1.4 NGCN Requirements

(R-NGCN-1) The NGN shall provide support for secure media transfer between NGCNs and NGNs.

(R-NGCN-2) An NGCN should permit media to be secured (encrypted, authenticated and integrity protected) transparently end-to-end or end to PSTN/ISDN gateway, except where requested or authorized intervention in media occurs.

(R-NGCN-3) An NGCN should be transparent to key management for the purpose of media security to take place between the end devices (or end device to PSTN/ISDN gateway), with cryptographic evidence that the peer involved in key exchange or key agreement is the expected communication partner.

(R-NGCN-4) An NGCN should be transparent to the end-to-end encryption of any key exchange required for the purpose of media security.

4.15.2 IMS-based Media Security Requirements

Void.

NOTE: This clause may be further elaborated for the purposes of Release 2.

4.15.3 Non-IMS-based Media Security Requirements

Void.

NOTE: This clause may be further elaborated for the purposes of Release 2.

4.16 Security Requirements to Counter Unsolicited Communications

(R-UC-1) The NGN shall provide a means for NGN-users to report calls as UC.

(R-UC-2) Reports of UC made by NGN-users shall be auditable by the NGN.

(R-UC-3) The NGN should provide the ability for an affected user to request the rating of an UC call.

(R-UC-4) The NGN should provide the ability for an affected user to challenge the ratings made by the UC detection system.

(R-UC-5) 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-6) The NGN should provide a mechanism to convey the UC rating in the call signalling.

(R-UC-7) The NGN should provide a mechanism to allow variation in the call handling for calls with particular UC ratings.

4.17 Business communication security requirements

Void.

NOTE: This clause may be further elaborated for the purposes of Release 2.

4.17.1 General security requirements

Void.

4.17.2 Specific security requirements for NGN/NGCN interconnection

Void.

4.17.3 Specific security requirements for hosted enterprise services

Void.

4.17.4 Specific security requirements for business trunking application

Void.

4.17.4.1 Security requirements for (subscription-based) business trunking application

Void.

4.17.4.2 Security requirements for (peering-based) business trunking application

Void.

4.17.5 Specific security requirements for virtual leased line

Void.

4.18 NAT Traversal Security Requirements

(R-NAT TRAV-1) TISPAN NGN R2 NAT traversal shall support the traversal of the following type of NATs behaviour between the UE and the IMS Core Network:

- Endpoint Independent Mapping.
- Address Dependent Mapping.
- Address and Port Dependent Mapping.

(R-NAT TRAV-2) TISPAN NGN R2 NAT traversal shall support the following type of filtering behaviour between the UE and the IMS Core Network:

- Endpoint Independent Filtering.
- Address Independent Filtering.
- Address and Port Dependent Filtering.

(R-NAT TRAV-3) TISPAN NGN R2 NAT traversal shall support both inbound and outbound requests to and from Ues through one or more NAT device(s).

(R-NAT TRAV-4) TISPAN NGN R2 NAT traversal shall support uni-directional and bi-directional RTP traffic.

(R-NAT TRAV-5) TISPAN NGN R2 NAT traversal shall support TCP connections initiated externally and internally.

(R-NAT TRAV-6) TISPAN NGN R2 NAT traversal shall support residential networks.

(R-NAT TRAV-7) TISPAN NGN R2 NAT traversal shall support IPv4.

(R-NAT TRAV-8) TISPAN NGN R2 NAT traversal shall support IPv6.

(R-NAT TRAV-9) TISPAN NGN R2 NAT traversal shall support unicast traffic.

(R-NAT TRAV-10) TISPAN NGN R2 NAT traversal should minimize the number of messages that are transmitted solely for NAT traversal.

(R-NAT TRAV-11) TISPAN NGN R2 NAT traversal shall support multiple Ues (on one or more devices) behind a single NAT.

(R-NAT TRAV-12) TISPAN NGN R2 NAT traversal should minimize additional session setup delay.

(R-NAT TRAV-13) TISPAN NGN R2 NAT traversal shall support the traversal for IMS.

(R-NAT TRAV-14) TISPAN NGN R2 NAT traversal shall support SIP signalling encrypted with Ipsec.

(R-NAT TRAV-15) TISPAN NGN R2 NAT traversal shall take into account the scalability, complexity and compatibility with other relevant NGN requirements.

(R-NAT TRAV-16) Any solution recommended for NAT traversal shall not impact the inherent ability of TLS to operate across NAT.

4.19 Home Networking Security Requirements

The security attacks identified in the CPN TVRA that pose either a major or critical risk to the CNG, and thus the CPN, should be protected against by standard measures that operators and service providers of CNGs shall establish and apply a security policy for by default in deployed equipment.

NOTE: The following requirements are in addition to those applying to an NGN terminal.

4.19.1 Confidentiality requirements

(R-CPN-CR-1) For shared credentials and media on wireless connections between the CND and the CNG, the minimum confidentiality protocol shall be WPA2.

(R-CPN-CR-2) Internally to the CPN, a CNG transmitting private or other critical information (i.e. to a CND) shall protect the data from unauthorised disclosure.

(R-CPN-CR-3) 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 unauthorised disclosure.

(R-CPN-CR-4) The CNG shall detect the end of the life of the key used for cryptographic protection of the wireless communication between the CND and the CNG.

4.19.2 Identification, authentication and authorization requirements

(R-CPN-IAAR-1) A CPN-user or external NGN user attempting to invoke a CNG-mediated service, including transparent routing, shall be identified and authenticated by the CNG before being granted access to the service.

(R-CPN-IAAR-2) The CNG shall implement an authentication failure handling policy.

(R-CPN-IAAR-3) The CNG shall take action according to local authentication failure handling policy (which may include silently discarding the authentication and explicit failure notification, or in the case of a replay of credentials may include notification of the true owner of the credentials) upon detection of failure during identification, authentication and authorization.

(R-CPN-IAAR-4) The CNG should detect replayed user and/or device credentials.

(R-CPN-IAAR-5) When the CNG detects replayed user and/or device credentials, the CNG shall stop the relevant processes.

(R-CPN-IAAR-6) The CNG shall implement a privacy protection policy specifying as a minimum private and critical information.

(R-CPN-IAAR-7) When the CNG detects violation of the privacy protection policy the CNG shall discard all signalling, including signalling from the NGN.

(R-CPN-IAAR-8) The CNG shall implement an authorization management handling policy.

NOTE: This could be used to allow the CNG and the CPN to support parental control related functionalities limiting the use of the broadband connection on a user or time basis. Limitations on a content basis may be shared with devoted network servers.

(R-CPN-IAAR-9) On reception at the CNG of a message to access configuration information for update and detection of authorization failure the CNG shall reject the request and manage the failure in accordance with the CPN authorization management handling policy.

Where a CND invokes a session at the CNG the CNG shall record the association of session-id, invoking device identity and invoking user-id.

4.19.3 Integrity requirements

(R-CPN-IR-1) On transmission of management information from the CNG to a CND the CNG shall append a timestamp or sequence number to the outgoing message.

(R-CPN-IR-2) On reception at the CNG of a message containing management information the CNG shall extract the timestamp or sequence number and verify that the message has not been replayed.

(R-CPN-IR-3) On reception at the CNG of a message to access or update configuration information the CNG shall allow access only if the sender is an administrator.

(R-CPN-IR-4) On detection of a message integrity error at the CNG the CNG shall discard the message.

(R-CPN-IR-5) On indication received at the CNG of a resource allocation expiry the CNG shall delete all residual data associated with the invocation of the resource.

4.19.4 Availability and DoS protection requirements

(R-CPN-AR-1) On receipt of a valid (i.e. authorized) request for data stored in the CNG the CNG shall return the requested data to the requesting user.

(R-CPN-AR-2) On receipt of a valid (i.e. authorized) request for access to a CNG hosted service or application the CNG shall provide the requested service or application to the requesting user.

(R-CPN-AR-3) On detection of any system failure or discontinuity not specifically handled by other mechanisms the CNG shall revert to a known safe state.

4.19.5 Service protection and/or content protection software upgrade security requirements

Service protection and/or content protection software upgrade allows adaptation of a CND to the protection mechanisms used by a specific relevant stakeholder (in the secure SP and/or CP software upgrade IPTV model). As service protection and/or content protection is a pivotal element in the secure distribution of protected content, upgrading such part of the system needs to be protected against malicious parties trying to attack such upgrade procedure. The motivation for attackers may be diverse. Therefore the supporting software functions for the upgrade of CND's service and content protection functions (CND-SPF and CND-CPF) need to comply with the following security requirements:

(R-CPN-SPCP-1) The CND's software upgrade function shall offer means to proof the validity of the CND's trusted environment for service protection and/or content protection software upgrade.

(R-CPN-SPCP-2) The CND shall authenticate the relevant stakeholder to verify if it is entitled to perform an service protection and/or content protection software upgrade.

(R-CPN-SPCP-3) During the upgrade, all security sensitive data (especially keys, passwords, credentials) shall be transported confidentiality and integrity protected between the CND and the relevant stakeholder.

(R-CPN-SPCP-4) Before new service protection and/or content protection software upgrades (e.g. the upgrade of software in the CND-SPF or software in the CND-CPF) are installed or activated their authenticity (proof of origin and data integrity) and their validity (e.g. credentials) shall be verified.

(R-CPN-SPCP-5) Handover of the CND from one relevant stakeholder to another shall be performed in a manner that only an entitled relevant stakeholder may initiate an upgrade of the CND service protection and/or content protection relevant software (the stakeholder must be authenticated by the CND and authorized to do this).

(R-CPN-SPCP-6) The CND-SPF and CND-CPF shall be implemented in a trusted execution environment. Such an environment shall be tamperproof and contain a secure storage environment for security sensitive information that these protection systems need to store and which shall not be revealed outside the CND.

NOTE: The specification of the implementation of the CND's trusted environment for service protection and/or content protection software upgrade and the secure storage environment is outside the scope of TISPAN.

(R-CPN-SPCP-7) The service protection and/or content protection system(s) in the relevant stakeholder domain shall be offered the possibility to authenticate the service protection and/or content protection software that is in operation in the CND as being authentic software provided by the service protection and/or content protection provider.

4.20 H.248 Security Requirements

Void.

NOTE: This clause may be further elaborated for the purposes of Release 2.

5 NGN Security Release 2 Requirements Mapping

Clause 5 maps the security requirements identified in clause 4 to the NASS, RACS, IMS and PES subsystems as well as the Application Server and the interfaces they apply to. Clause 5 is intended as an informational clause to make it easier to trace requirements per interface and subsystem.

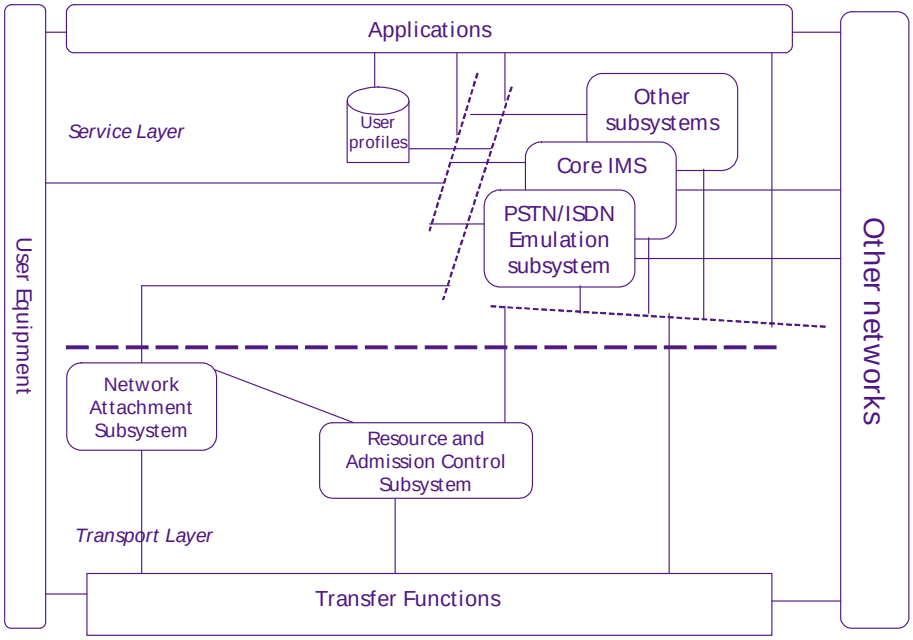


Figure 1: TISPAN NGN overall architecture

5.1 Network Access SubSystem (NASS)

Requirements related to NASS

Security Requirements	
(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.
(R-AA- 26)	In case the CNG is a bridge, each UE shall authenticate with the NASS as the IP realm in the CPN is known to the Access Network.
(R-AA- 3)	In non-early deployment scenarios, IMS authentication shall be independent from access authentication.
(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-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.
(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- 29)	Caller id and location information shall be stored according to the Common European regulatory framework by the EMTEL Service Provider. Caller ID and location information shall be validated by the EMTEL Service Provider.
(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- 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-IR- 2)	An access identity shall be used for access authentication. This identity may or may not be used for other purposes.
(R-IR- 3)	The line ID shall be possible to use for line authentication.
(R-CD- 2)	Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [3].
(R-CD- 3)	All NDS/IP traffic shall pass through a SEGF (Security Gateway Function) before entering or leaving the security domain. IMS operators shall operate NDS/IP Za interface between SEGFs according to TS 133 210 [3].
(R-CD- 7)	In case access authentication is independent from IMS authentication.
(R-CD- 8)	In the case where IMS authentication is linked to access line authentication the underlying access technology shall provide protection of NGN signalling and user data.
(R-CD- 12)	All data related to configuring the UE through the e3 reference point shall be protected against loss of confidentiality and against loss of integrity.
(R-CD- 13)	Integrity protection of signalling, control communications and of stored data shall be provided.
(R-CD- 18)	Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.

Security Requirements
(R-CD- 19) Confidentiality of signalling and control messages shall be enforced if required by the application or in environments where the security policy demands confidentiality. The mechanism should allow a choice in the algorithm to be used.
(R-CD- 22) It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.
(R-P- 1) It shall be possible to protect the network topology from exposure toward other domains. It shall also be possible for a security domains to define and implement protection against traffic analysis for signalling and management protocols.
(R-P- 2) User location and usage patterns shall be kept from unwanted disclosure.
(R-P- 3) It shall be possible to protect the confidentiality of user identity data.
(R-P- 5) NGN shall support the specific case where the destination party has an override right (e.g. emergency communication sessions), and the originating party identity is provided to the destination party independent whether or not this communication session is anonymous.
(R-P- 7) The NGN shall support mechanisms for the network operator to guarantee 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- 8) The NGN shall provide mechanisms that allow to present the identity of the session originator, if this is not restricted by the session originator.
(R-KM- 3) The key management mechanism must be able to traverse a NAT/NATP device.
(R-NF- 1) NGN security protocols shall work with commonly-used firewalls and shall work in environments with NAT/NATP.
(R-NF- 2) Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.
(R-AD- 1) Mechanisms shall be provided to mitigate denial-of-service attacks.
(R-AD- 2) Provide access control mechanisms to ensure that authorized users only can access the service.
(R-AD- 3) It shall be possible to prevent intruders from restricting the availability of services by logical means.
(R-AD- 4) Availability of and accuracy of location information shall be provided for the EMTEL services.
(R-AD- 5) Availability of EMTEL PSAPs shall not be decreased by DoS attacks. EMTEL PSAPs shall be able to reconnect.
(R-AS- 1) The TISPAN NGN shall provide guidance for evaluating and certifying NGN equipment and systems.
(R-AS- 2) Security implications of potential misuse of protocols used in NGN shall be documented through a TVRA. This enables users to assess the security they need before deploying the given protocol.

5.2 Resource and Admission Control Subsystem (RACS)

Requirements related to RACS

Security Requirements
(R-AA- 27): RACS and AF shall be mutually authenticated prior to resource authorization.
(R-AA- 27A): AF and SPDF in RACS shall be able to mutually identify each other when performing the authentication.
(R-CD- 17): RACS shall ensure integrity of all policy related resource information exchanged between NASS and RACS. NOTE 1: This requires that RACS is the validator of the integrity of the data exchanged, and that NASS is the generator of the integrity check data.
(R-CD- 18): Data integrity validation in RACS shall be enforced using either Message Digest (MD) or cryptographic Message Authentication Code (MAC) with keys derived from the unique application layer identities of AF and SPDF (as specified in requirement R-AA-28). NOTE 2: Unique application layer identities as specified in requirement R-AA-28 are a pre-requisite for R-CD-17 and R-CD-18.
(R-AA- 28): RACS and CPN shall be mutually authenticated prior to resource authorization. NOTE: For emergency services alternative procedures are required.
(R-CD- 24): RACS shall ensure integrity of all policy related resource information exchanged between CPN and RACS. NOTE 1: This requires that RACS is the validator of the integrity of the data exchanged, and that CPN is the generator of the integrity check data.
(R-CD- 23): RACS shall ensure confidentiality of all policy related resource information exchanged between CPN and RACS.
(R-P- 1) It shall be possible to protect the network topology from exposure toward other domains. It shall also be possible for a security domains to define and implement protection against traffic analysis for signalling and management protocols.
(R-P-15): The CPN transmitting information to the RACS shall not disclose CPN internal (private or other critical) information to the RACS.

5.3 The Core IP Multimedia Subsystem (IMS)

Requirements related to Core IMS

Security Requirements
(R-AA- 1) Access to NGN networks, services, and applications shall be provided for authorized users only.
(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.
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.
(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- 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.
(R-AA- 28) Authentication of NGN users and authentication of NGN terminals shall be separate.
(R-AA- 29) Caller id and location information shall be stored according to the Common European regulatory framework by the EMTEL Service Provider. Caller ID and location information shall be validated by the EMTEL Service Provider.
(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.

Security Requirements	
(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.
(R-IR- 1)	It shall be possible to implicitly register IMPU(s). The implicitly registered IMPU(s) all belong to the same Service Profile. All the IMPU(s) being implicitly registered shall be delivered by the HSS to the S-CSCF and subsequently to the P-CSCF. The S-CSCF shall regard all implicitly registered IMPU(s) as registered IMPU(s).
(R-IR- 2)	An access identity shall be used for access authentication. This identity may or may not be used for other purposes.
(R-CD- 1)	Confidentiality and integrity of IMS signalling shall be applied in a hop-to-hop fashion. (UE-to-P-CSCF and among other Nes).
(R-CD- 2)	Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [3].
(R-CD- 3)	All NDS/IP traffic shall pass through a SEGF (Security Gateway Function) before entering or leaving the security domain. IMS operators shall operate NDS/IP Za interface between SEGFs according to TS 133 210 [3].
(R-CD- 4)	Security shall be provided within the network domain for the Cx interface.
(R-CD- 5)	An ISIM based solution for IMS access security (authentication, confidentiality and integrity protection) of signalling to and from the user, shall be supported.
(R-CD- 6)	Secure link shall be provided between UE and the P-CSCF for protection of the Gm reference point.
(R-CD- 7)	In case access authentication is independent from IMS authentication.
(R-CD- 8)	In the case where IMS authentication is linked to access line authentication the underlying access technology shall provide protection of NGN signalling and user data.
(R-CD- 9)	ISIM specific information shall be updated in a secure manner.
(R-CD- 13)	Integrity protection of signalling, control communications and of stored data shall be provided.
(R-CD- 14)	It shall be possible to ensure the origin, integrity and freshness of authentication data, particularly of the cipher key.
(R-CD- 15)	Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling.
(R-CD- 16)	Integrity protection between Network Elements (e.g. between CSCFs, and between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [3].
(R-CD- 18)	Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.
(R-CD- 19)	Confidentiality of signalling and control messages shall be enforced if required by the application or in environments where the security policy demands confidentiality. The mechanism should allow a choice in the algorithm to be used.
(R-CD- 20)	IMS specific confidentiality protection shall be provided for the SIP signalling between UE and P-CSCF.
(R-CD- 21)	Confidentiality protection between Network Functions (e.g. between CSCFs, or between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [3].
(R-CD- 22)	It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.
(R-P- 1)	It shall be possible to protect the network topology from exposure toward other domains. It shall also be possible for a security domains to define and implement protection against traffic analysis for signalling and management protocols.
(R-P- 2)	User location and usage patterns shall be kept from unwanted disclosure.
(R-P- 3)	It shall be possible to protect the confidentiality of user identity data.
(R-P- 4)	Anonymous communication sessions shall be supported in NGN either in a permanent mode or in a temporary mode communication by call. In this case the originating party identity shall not be presented to the destination party. The network to which the destination party is connected to is responsible to handle this service.
(R-P- 5)	NGN shall support the specific case where the destination party has an override right (e.g. emergency communication sessions), and the originating party identity is provided to the destination party independent whether or not this communication session is anonymous.
(R-P- 6)	The Anonymous Communications Rejection (ACR) simulation service shall allow the served user to reject incoming communication from users or subscribers who have restricted the presentation of their originating identity according to the OIR simulation service.
(R-P- 7)	The NGN shall support mechanisms for the network operator to guarantee 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- 8)	The NGN shall provide mechanisms that allow to present the identity of the session originator, if this is not restricted by the session originator.
(R-P- 9)	The privacy aspect of presence information and the need for authorization before providing presence information shall be configurable by the user (i.e. presentity).
(R-P- 10)	A principal of a presentity shall, at any time, be able to control to whom, for how long and what (all or part of) presence information of the presentity is provided, and a principal of a watcher shall, at any time, be able to control to whom, for how long and what (all or part of) watcher information of the watcher is provided

Security Requirements	
(R-P- 11)	Any services using the presence information shall ensure privacy agreement before releasing presence information. The presence service does not address deployment specific issues (e.g. where agreements are stored or how they are negotiated). It only gives requirements for privacy management.
(R-P- 12)	It shall be possible for the sender of the message to request to hide its public ID from the recipient.
(R-P- 13)	Users may select the Identity presented when starting a session or sending a message. It shall be possible to verify this identity and to initiate a session or message in reply.
(R-KM- 1)	Key management and key distribution between SEGFs shall comply to the Network Domain Security TS 133 210 [3].
(R-KM- 2)	The UE and the AS shall be able to resume a previously established secure session.
(R-KM- 3)	The key management mechanism must be able to traverse a NAT/NATP device.
(R-NF- 1)	NGN security protocols shall work with commonly-used firewalls and shall work in environments with NAT/NATP.
(R-NF- 2)	Filters to screen the IP packets to restrict/grant access to specific bearer streams shall be supported.
(R-NF- 3)	The SEGFs may include filtering policies and firewall functionality not required in TS 133 210 [3].
(R-AD- 1)	Mechanisms shall be provided to mitigate denial-of-service attacks.
(R-AD- 2)	Provide access control mechanisms to ensure that authorized users only can access the service.
(R-AD- 3)	It shall be possible to prevent intruders from restricting the availability of services by logical means.
(R-AD- 4)	Availability of and accuracy of location information shall be provided for the EMTEL services.
(R-AD- 5)	Availability of EMTEL PSAPs shall not be decreased by DoS attacks. EMTEL PSAPs shall be able to reconnect.
(R-AS- 1)	The TISPAN NGN shall provide guidance for evaluating and certifying NGN equipment and systems.
(R-AS- 2)	Security implications of potential misuse of protocols used in NGN shall be documented through a TVRA. This enables users to assess the security they need before deploying the given protocol.

5.4 The PSTN/ISDN Emulation subsystem (PES)

Requirements related to PES

Security Requirements
(R-AA- 27) A media gateway controller must be able to handle authentication of multiple media gateways, i.e. to maintain multiple security associations with different media gateways.
(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-CD- 2) Network Domain Security (NDS) shall be provided at the network layer and comply to TS 133 210 [3].
(R-CD- 3) All NDS/IP traffic shall pass through a SEGF (Security Gateway Function) before entering or leaving the security domain. IMS operators shall operate NDS/IP Za interface between SEGFs according to TS 133 210 [3].
(R-CD- 8) In the case where IMS authentication is linked to access line authentication the underlying access technology shall provide protection of NGN signalling and user data.
(R-CD- 13) Integrity protection of signalling, control communications and of stored data shall be provided.
(R-CD- 16) Integrity protection between Network Elements (e.g. between CSCFs, and between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [3].
(R-CD- 18) Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.
(R-CD- 19) Confidentiality of signalling and control messages shall be enforced if required by the application or in environments where the security policy demands confidentiality. The mechanism should allow a choice in the algorithm to be used.
(R-CD- 21) Confidentiality protection between Network Functions (e.g. between CSCFs, or between CSCFs and the HSS) shall rely on mechanisms specified by Network Domain Security in TS 133 210 [3].
(R-CD- 22) It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.
(R-P- 1) It shall be possible to protect the network topology from exposure toward other domains. It shall also be possible for a security domains to define and implement protection against traffic analysis for signalling and management protocols.
(R-P- 2) User location and usage patterns shall be kept from unwanted disclosure.
(R-P- 3) It shall be possible to protect the confidentiality of user identity data.
(R-P- 4) Anonymous communication sessions shall be supported in NGN either in a permanent mode or in a temporary mode communication by call. In this case the originating party identity shall not be presented to the destination party. The network to which the destination party is connected to is responsible to handle this service.
(R-P- 5) NGN shall support the specific case where the destination party has an override right (e.g. emergency communication sessions), and the originating party identity is provided to the destination party independent whether or not this communication session is anonymous.
(R-P- 7) The NGN shall support mechanisms for the network operator to guarantee 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- 8) The NGN shall provide mechanisms that allow to present the identity of the session originator, if this is not restricted by the session originator.
(R-AD- 2) Provide access control mechanisms to ensure that authorized users only can access the service.
(R-AD- 4) Availability of and accuracy of location information shall be provided for the EMTEL services.
(R-AS- 1) The TISPAN NGN shall provide guidance for evaluating and certifying NGN equipment and systems.
(R-AS- 2) Security implications of potential misuse of protocols used in NGN shall be documented through a TVRA. This enables users to assess the security they need before deploying the given protocol.

5.5 Application Server (AS)

Clause 5.5 lists the security requirements related to the Application Systems.

NOTE: This is not a separate subsystem, but has been included to make it easier to track AS related requirements.

Security Requirements
(R-AA- 1) Access to NGN networks, services, and applications shall be provided for authorized users only.
(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- 8) NGN relevant ISIM specific information shall be protected against unauthorized access or alteration.
(R-AA- 12) Transmitted passwords shall be sufficiently protected; e.g. by encryption or other techniques.
(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.
(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-CD- 10) It shall be possible to protect sensitive data (such as Presence information and notifications) from attacks (e.g. eavesdropping, tampering, and replay attacks).
(R-CD- 13) Integrity protection of signalling, control communications and of stored data shall be provided.
(R-CD- 17) Data integrity shall be supported between the UE and the Application Server.
(R-CD- 18) Confidentiality of communications should be achieved by cryptographic encryption. Confidentiality of stored data shall be achieved by cryptographic encryption or by access controls.
(R-CD- 19) Confidentiality of signalling and control messages shall be enforced if required by the application or in environments where the security policy demands confidentiality. The mechanism should allow a choice in the algorithm to be used.
(R-CD- 22) It shall be possible to protect the confidentiality of user-related data which is stored or processed by a provider.
(R-P- 2) User location and usage patterns shall be kept from unwanted disclosure.
(R-P- 3) It shall be possible to protect the confidentiality of user identity data.
(R-P- 7) The NGN shall support mechanisms for the network operator to guarantee 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- 8) The NGN shall provide mechanisms that allow to present the identity of the session originator, if this is not restricted by the session originator.
(R-P- 9) The privacy aspect of presence information and the need for authorization before providing presence information shall be configurable by the user (i.e. presentity).
(R-P- 10) A principal of a presentity shall, at any time, be able to control to whom, for how long and what (all or part of) presence information of the presentity is provided, and a principal of a watcher shall, at any time, be able to control to whom, for how long and what (all or part of) watcher information of the watcher is provided.
(R-P- 11) Any services using the presence information shall ensure privacy agreement before releasing presence information. The presence service does not address deployment specific issues (e.g. where agreements are stored or how they are negotiated). It only gives requirements for privacy management.
(R-KM- 2) The UE and the AS shall be able to resume a previously established secure session.
(R-NF- 1) NGN security protocols shall work with commonly-used firewalls and shall work in environments with NAT/NATP.
(R-AD- 2) Provide access control mechanisms to ensure that authorized users only can access the service.
(R-AS- 1) The TISPAN NGN shall provide guidance for evaluating and certifying NGN equipment and systems.
(R-AS- 2) Security implications of potential misuse of protocols used in NGN shall be documented through a TVRA. This enables users to assess the security they need before deploying the given protocol.

Annex A (informative): Bibliography

- ETSI TS 133 141: "Universal Mobile Telecommunications System (UMTS); Presence service; Security (3GPP TS 33.141)".
- ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); H.248 Profile for controlling Access and Residential Gateways".
- ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 2 Lawful Interception; Stage 1 and Stage 2 definition".
- ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); LTE; Network Domain Security (NDS); Authentication Framework (AF) (3GPP TS 33.310)".
- ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)".

Annex B:
Void

Annex C (informative): Trust domains in NGN

NOTE: The term "trust" is not defined in ISO 27000 [i.6], "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

C.1 Definition of trust for the NGN - analysis

ISO 15408-1 [i.1] does not directly define trust but does define a trusted channel and a trusted path. ISO 15408-2 [i.3] defines functional capabilities (used in the functional requirement layer of the TISPAN Security requirements method in TR 187 011 [i.7]) that may be used to further refine trust in the NGN.

Trusted channel: a means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path: a means by which a user and a TSF can communicate with necessary confidence to support the TSP.

For the NGN it is assumed that the TSF is the NGN and the TSP are those policies required to assure security of the NGN.

In the NGN trust describes the relationship between entities where there is a verified assertion of identity and authority between the entities. As identified in TR 187 010 [i.8] the identity model consists of 3 elements:

- Principal
  - Often synonymous with the end-user and in telecommunications protocols viewed as an electronic or digital representation of the end-user.

NOTE: In Subscriber Management within the NGN the principal may be a human rather than a representation of a human as end-user.

- Identity Provider (IdP)
  - The primary role of the IdP in IdM is to authenticate the Principal and to provide an assertion of this authentication to the Relying Party.
- Relying Party (RP)
  - The RP provides a service to the Principal; to this end, the Principal may authenticate to the RP, but, the RP is also willing to rely on an assertion provided by the IdP.

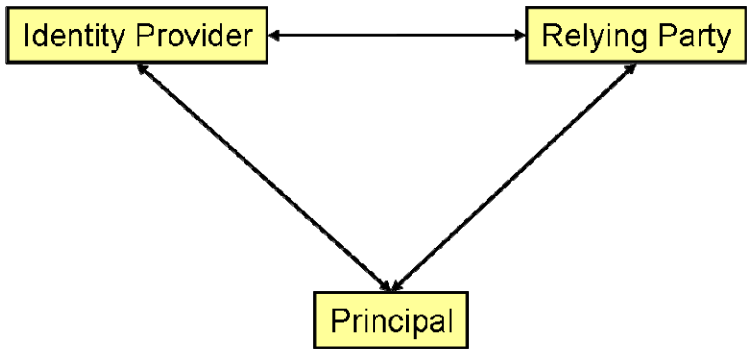


Figure C.1: Roles (or entities) in Authentication, SSO and Identity Federation scenarios (from TR 187 010 [i.8])

The establishment of trust requires that the relying party accepts the assertion of identity provided by the identity provider prior to offering service to the principal.

In instances where the RP is in a separate NGN from the IdP, e.g. when an NGCN is communicating with an NGN where the NGN is acting as the RP and the NGCN as the IdP, the assertion of identity may be achieved using authentication mechanisms where the RP and IdP act together to complete authentication (i.e. authentication cannot be performed solely by the RP based on assertions of the principal).

C.2 Requirements for creation of trusted channel

Following the model for definition of requirements in TR 187 011 the following assertions are made.

C.2.1 Functional security requirements for trusted channel in the NGN

The functional requirements are stated as refinements of ISO 15408-2 [i.3] functional capabilities.

The NGN provides a communication channel between itself and a remote NGN/NGCN that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure (from ISO 15408-2 FTP_ITC.1.1 [i.3]).

The NGN permits the NGN CSCF entity to initiate communication via the trusted channel (from ISO 15408-2 FTP_ITC.1.2 [i.3]).

The NGN permits the NGCN CSCF entity to initiate communication via the trusted channel (from ISO 15408-2 FTP_ITC.1.2 [i.3]).

C.3 Existing NGN capabilities

RFC 3324 [i.4]: "Short Term Requirements for Network Asserted Identity".

RFC 3325 [i.5]: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

The P-Asserted Identity (PAI) is used to indicate that the SIP proxy has taken steps to validate the identity contained in the PAI header. In mapping to the identity model in clause C.1 the SIP-Proxy acts as the relying party, and passes that information to a receiving SIP-UA that also acts as a relying party.

The assertions in RFC 3324 [i.4] are that PAI when present in messages indicates the following:

- INVITE - the calling user;
- 180 response - the ringing user;
- 200 OK - the user who answered the call.

The behaviour of a SIP proxy, and of a SIP UAS, is determined by the ability of the SIP proxy or SIP UAS to identify a trust domain. However, the PAI specification does not indicate how trust is assured for PAI.

Annex D (informative): Security Objective Categories

Security objectives are high-level statements of the overall security goals of a system. Security objectives are categorized into seven categories according to the seven security attributes as defined in ISO/IEC TR 13335 [i.10].

D.1 Security Objective Categories Definitions

confidentiality: (or secrecy) means that information is made available or disclosed only to authorized individuals, entities or processes [i.10].

Integrity: means that information is not destroyed or altered in an unauthorized manner and that the system performs its intended function in an unimpaired manner free from deliberate or accidental unauthorized manipulation of the system [i.10].

Availability: means that system services are accessible and usable on demand by an authorized entity [i.10].

Authenticity: ensures that the identity of a subject or resource is the one claimed [i.10].

Accountability: means that actions of an entity may be traced uniquely to the entity [i.10].

Non-repudiation: is the ability to prove that an action or event has taken place in order to prevent later repudiation of this event or action [i.10].

Reliability: The property of consistent intended behaviour and results [i.10].

Annex E (informative): Security Objectives

This annex lists the security objectives derived from TR 187 002 [i.11]. The security objectives are categorized according to the security objective categories definitions given in Annex D and structured according to the recommendations of TR 187 011 [i.7].

E.1 General objectives

1) Access to services should only be granted to users with appropriate authorization
2) The identity of an user should not be compromised by any action of the system
3) No action of the system should make a user liable to be the target of identity crime
4) No change in the ownership, responsibility, content or collection of personal data pertaining to a user should occur without that user's consent or knowledge
5) Personal data pertaining to a user should be collected by the system using legitimate means only
6) An audit trail of all transactions having an impact on personal data pertaining to users should be maintained within the system

E.2 Security objective category confidentiality

OBJ-CONF-01	Information sent to or from a registered user of an NGN should not be revealed to any unauthorized party
01a	Media sent between registered NGN users and the NGN (end to middle media path) should not be revealed to any unauthorized party
01b	Media sent between two registered NGN users (end to end point to point media path) should not be revealed to any unauthorized party
01c	Signalling between a registered NGN user and the NGN should not be revealed to any unauthorized party
01d	Signalling between entities within the NGN (intra NGN signalling) should not be revealed to any unauthorized party
01e	Signalling between NGNs (inter NGN signalling) should not be revealed to any unauthorized party
OBJ-CONF-02	Information held within the functional entities that constitute an NGN should be protected from unauthorized access
02a	Details relating to the identity and service capabilities of an NGN user should not be revealed to any unauthorized 3rd party within the NGN or its connected networks
02b	Management Information sent to or from an NGN should not be revealed to any unauthorized party
02c	Management Information held within an NGN should be protected from unauthorized access
OBJ-CONF-03	Data gathered by the NGN should be maintained in accordance with relevant laws on data protection

E.3 Security objective category integrity

OBJ-INT-01 An NGN should ensure that unauthorized modification of media streams is prevented

OBJ-INT-02 An NGN should ensure that unauthorized modification of signalling is prevented.

OBJ-INT-03 An NGN should ensure protection of media streams from unauthorized replay

OBJ-INT-04 An NGN should ensure protection of signalling from unauthorized replay

OBJ-INT-05 An NGN should ensure protection of media streams from unauthorized replay

OBJ-INT-06 An NGN should ensure protection of signalling from unauthorized data injection

OBJ-INT-07 An NGN should ensure protection of media streams from unauthorized data injection

E.4 Security objective category availability

OBJ-AVL-01 An NGN should ensure that any service offered is available within the terms of any agreement with the service user

E.5 Security objective category authenticity

OBJ-AUTH-01 It should not be possible for an unauthorized user to pose as an authorized user when communicating with an application or other user of an NGN

OBJ-AUTH-02 It should not be possible for an NGN to receive and process management and configuration information from an unauthorized user

OBJ-AUTH-03 An NGN user should be able to authenticate the source of an incoming media stream

OBJ-AUTH-04 An NGN entity should be able to authenticate the source of an incoming signal

OBJ-AUTH-05 An NGN entity should be able to authenticate the identity of any other NGN entity that it communicates with

Annex F (informative): Change history

Date	WG Doc.	CR	Rev	CAT	Title / Comment	Current Version	New Version
09-01-09	19tTD036r2	01		F	Early deployments for NGN R3	3.0.0	3.1.0
09-01-09	19tTD092r2	02		B	Addition of security objective categories definitions to WI07036	3.0.0	3.1.0
09-02-09	20WTD045r2	03		B	Security objectives from TR 187 002	3.0.0	3.1.0
17-07-09	21bTD146r2	05		B	Requirement for open IPTV protection framework	3.1.0	3.2.0
22-09-09	22WTD087r3	04		B	Addition of requirements arising from CPN TVRA to home network section	3.1.0	3.2.0
14-12-09	23WTD197r1	06		B	Service Protection new requirements	3.2.0	3.3.0
02-05-10	TISPAN07(10) 0032r1	07		B	insert CPN-RACS requirements	3.3.0	3.4.0
21-10-10	TISPAN07(10) 0156	09		B	CR on service protection and/or content protection software upgrade security requirements	3.4.0	3.5.0
21-10-10	TISPAN07(10) 0151r1	10		B	Addition of specific objectives to TS 187 001	3.4.0	3.5.0
30-11-10	TISPAN07(10) 0172r1	11		D	Removal of annex B	3.5.0	3.6.0
02-12-10	TISPAN07(10) 0197r3	12		F	Adding security requirements arising from NASS TVRA	3.5.0	3.6.0
					Addition of Change history table	3.6.0	3.7.0

History

Document history		
V1.1.1	March 2006	Publication
V2.1.5	October 2008	Publication
V3.7.1	March 2011	Publication