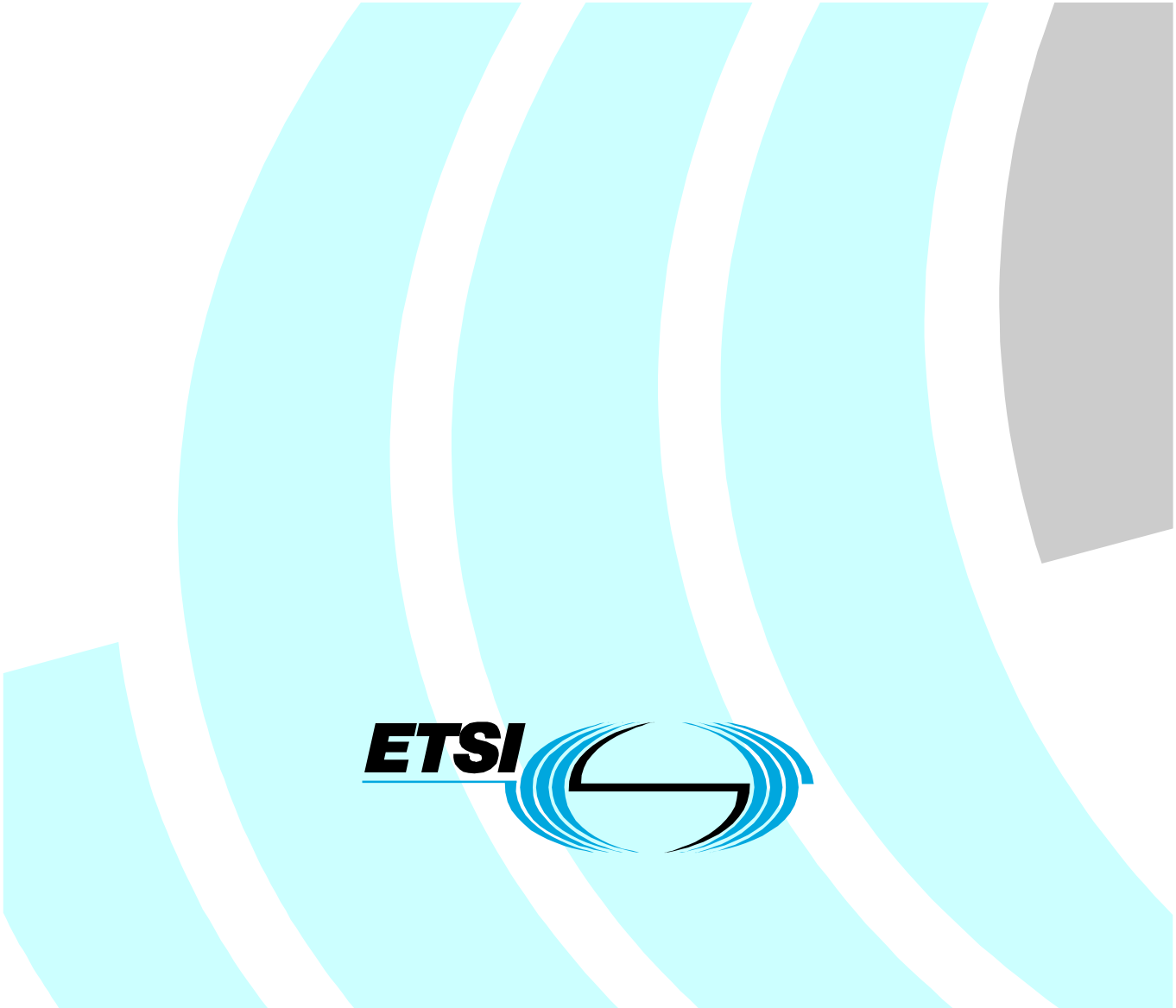
ETSI TS 187 001 V1.1.1 (2006-03)

Technical Specification

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



Reference
DTS/TISPAN-07014-NGN-R1

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 R1 security is defined by the security requirements in the present document, while the architectural aspects and stage 2 implementations outline are covered in the Security Architecture for R1 (TS 187 003 [1]).

1 Scope

The present document defines the security requirements pertaining to TISPAN NGN Release 1. 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

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[2] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)".

[3] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210)".

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

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

3.2 Abbreviations

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

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AA	Authentication & Authorization
ACR	Anonymous Communications Rejection
AF	Application Function
ALG	Application Layer Gateway
AP	Authentication Proxy
AS	Application Server
CNG	Customer Network Gateway
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSCF	Call Session Control Function
DoS	Denial-of-Service
HSS	Home Subscriber Server
ID	IDentity
IKE	Internet Key Exchange
IMPU	IMS PUblic user ID
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISIM	IMS Subscriber Identity Module
NAF	operator controlled Network Application Function
NAPT	Network Address and Port Translation
NASS	Network Access SubSystem
NAT	Network Address Translation
NDS	Network Domain Security
NGN	Next Generation Network
P-CSCF	Proxy - Call Session Control Function
PES	PSTN/ISDN Emulation Subsystem
RACS	Resource Admission Control Subsystem
S-CSCF	Serving - Call Session Control Function
SEGF	SEcurity Gateway Functions
SIP	Session Initiation Protocol
TE	Terminal Equipment
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
TS	Technical Specification
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System

4 Security Requirements

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

High level Objectives

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

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

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

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

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

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

4.1 Security Policy Requirements

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

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

(R-SP- 2): Security mechanisms and other parameters beyond default security mechanisms shall be configurable. This shall be static for NNI interface and may be negotiated for UNI interfaces. The security mechanism negotiation shall have a certain minimum level to be defined by the security domain; e.g. avoid bidding-down attacks. Users shall be able to reject communications that do not conform to their minimum security policy.

(R-SP- 3): The security mechanisms shall be partitioned such that the functions of authentication, data integrity, replay detection, and confidentiality may be implemented and selected independently of each other, insofar as this makes sense.

(R-SP- 4): The UE shall always offer encryption algorithms for P-CSCF to be used for the session and the P-CSCF policy shall define whether to use encryption or not.

(R-SP- 5): The UE and the P CSCF shall negotiate the integrity algorithm that shall be used for the session.

(R-SP- 6): The policy of the HN shall be used to decide if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles.

(R-SP- 7): The security gateway functions (SEGF) shall be responsible for enforcing security policies for the interworking between networks.

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

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

4.2 Authentication, Authorization, Access Control and Accountability Requirements

General Access authentication

(R-AA- 1): Access to NGN networks, services, and applications shall be provided for authorized users only.

(R-AA- 2): NGN R1 IMS authentication shall support early deployment scenarios (with support for legacy equipments).

(R-AA- 3): In non-early deployment scenarios, IMS authentication shall be independent from access authentication.

(R-AA- 4): An ISIM shall be used to access any IMS service, however, exceptions may be allowed for emergency calls and early deployment scenarios.

(R-AA- 5): ISIM based Authentication between the IMS-subscriber and the network shall comply to the authentication part of Access Security for IP-based services TS 133 203 [2].

(R-AA- 6): ISIM based Re-authentication of an IMS-subscriber shall comply to the authentication part of Access Security for IP-based services TS 133 203 [2].

(R-AA- 7): It shall be possible to prevent the use of a particular ISIM to access NGN networks and services and it should be possible to revoke a specific ISIM.

(R-AA- 8): NGN relevant ISIM specific information shall be protected against unauthorized access or alteration.

(R-AA- 9): User authentication may either be hardware-based (for 3GPP UE: ISIM; i.e. proof by possession of a physical token) or be software-based (i.e. proof by knowledge of some secret information).

Early Deployments

(R-AA- 10): User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as a 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.

(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) 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): As the interface between the Application Function (AF) and RACS can be inter-operator, the RACS shall authenticate and authorize the Application Function (AF).

Other Specific Requirements

(R-AA- 28): 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- 29): Authentication of NGN users and authentication of NGN terminals shall be separate.

(R-AA- 30): 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 aims 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): The Rq and Gq' reference points shall provide mechanism to assure security of the information exchanged.

Other Specific Requirements

(R-CD- 12): All data related to configuring the UE through the e3 if 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.

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.

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.

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.

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

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

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 [4] shall be followed when defining or selecting cryptographic algorithms in TISPAN.

5 NGN Security Release 1 Requirements Mapping

Clause 5 maps the security requirements identified in clause 4 to the different subsystems as well as the interfaces they applies to. Clause 5 is intended as an informational clause to make it easier to trace requirements per interface and subsystem.

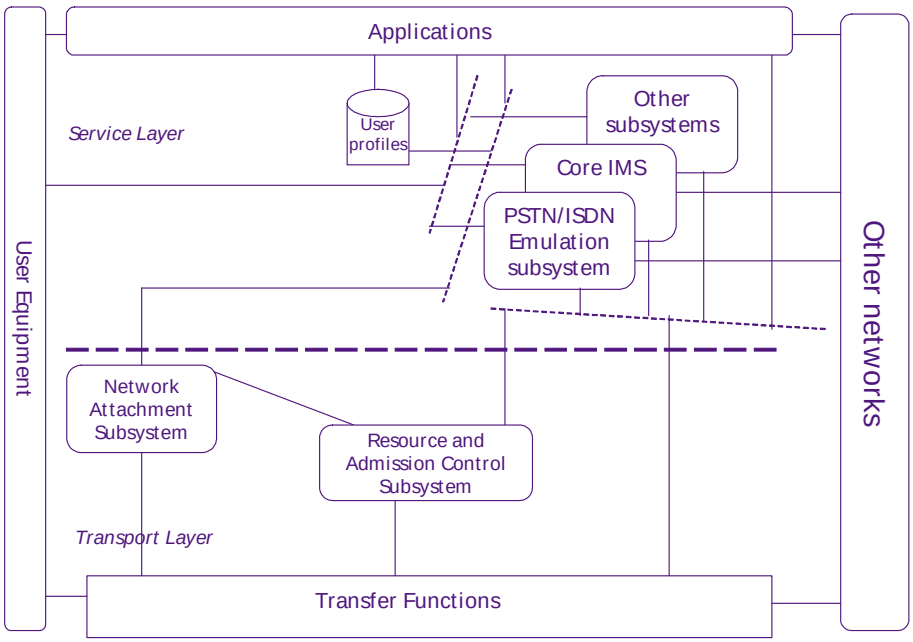


Figure 1: TISPAN NGN overall architecture

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) 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.

Security Requirements
(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.
(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- 30): 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 if 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.
(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).

Security Requirements
(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): As the interface between the Application Function (AF) and RACS can be inter-operator, the RACS shall authenticate and authorize the Application Function (AF).
(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- 11): The Rq and Gq' reference points shall provide mechanism to assure security of the information exchanged.
(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.
(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-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.

5.3 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.
(R-AA- 9): User authentication may either be hardware-based (for 3GPP UE: ISIM; i.e. proof by possession of a physical token) or be software-based (i.e. proof by knowledge of some secret information).
(R-AA- 10): User Authentication to the NGN IMS using SIP Digest mechanisms shall be supported as a 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.
(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- 29): Authentication of NGN users and authentication of NGN terminals shall be separate.
(R-AA- 30): 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.
(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.

Security Requirements
(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
(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.

Security Requirements
(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- 28): 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.

Security Requirements
(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)".

History

Document history		
V1.1.1	March 2006	Publication