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

Technical Specification

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

Reference

RTS/TISPAN-07026-NGN-R2

Keywords

security, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2008.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

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

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

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

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
    - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
    - for informative references.

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

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ISO 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.2] IEEE 802.1X: "Port Based Network Access Control".

[i.3] ISO 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components".

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

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

[i.6] ETSI ES 283 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); H.248 Profile for controlling Access and Residential Gateways".

[i.7] ETSI TS 187 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Lawful interception functional entities, information flow and reference points".

[i.8] ETSI TS 133 310: "Universal Mobile Telecommunications System (UMTS); Network domain security; Authentication framework (NDS/AF) (3GPP TS 33.310)".

[i.9] ETSI TS 133 234: "Universal Mobile Telecommunications System (UMTS); 3G security; Wireless Local Area Network (WLAN) interworking security (3GPP TS 33.234)".

[i.10] ISO 27000: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

[i.11] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.12] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity imanagement and their resolution in the NGN".

[i.13] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

3.2 Abbreviations

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

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

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

4 Security Requirements

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

High level Objectives

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

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

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

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

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

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

4.1 Security Policy Requirements

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

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

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

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

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

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

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

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

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

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

4.2 Authentication, Authorization, Access Control and Accountability Requirements

General Access authentication

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

(R-AA- 2) NGN R1 and R2 IMS authentication shall support early deployment scenarios (with support for legacy equipments), although it is optional for operators to deploy such scenarios.

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

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

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

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

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

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

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

Early Deployments

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

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

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

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

NOTE 1: The two special early deployment scenarios are (also referred to as NASS Bundled authentication):
(A). IMS authentication is linked to access line authentication (no nomadicity).
(B). IMS authentication is linked to access authentication for IP Connectivity (limited nomadicity can be provided).

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

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

Ut Interface

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

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

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

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

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

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

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

NASS

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

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

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

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

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

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

(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.

Other Specific 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-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.

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) 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- 23) RACS shall ensure integrity of all information exchanged over the e4 reference point.

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

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 [4] 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).

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.

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

5.15.1.1 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.

5.15.1.2 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

5.15.1.3 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.

5.15.1.4 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 IP v4.

(R-NAT TRAV-8) TISPAN NGN R2 NAT traversal shall support IP v6.

(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

Void.

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

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.

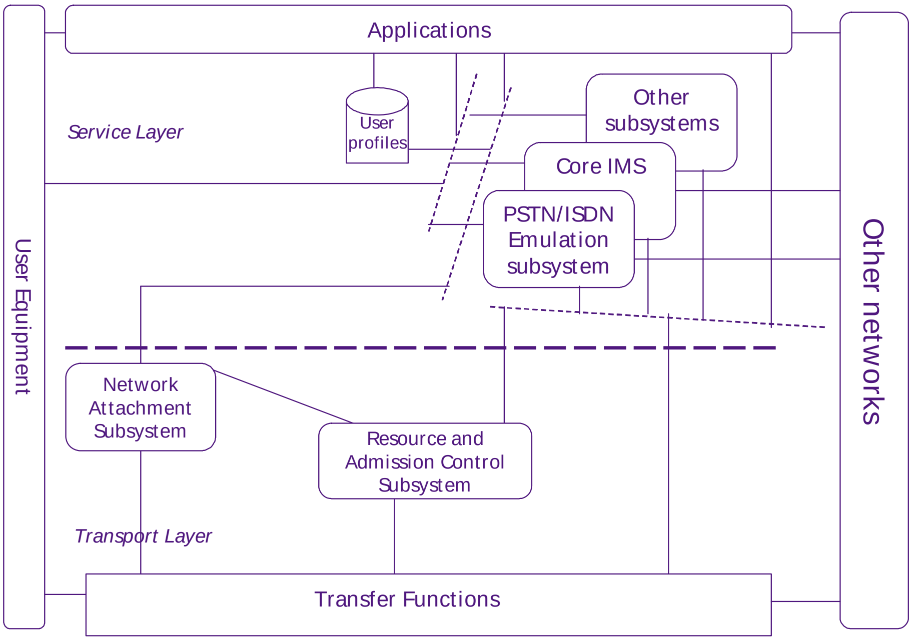

Figure 1: TISPAN NGN overall architecture

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) 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.
(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.
(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.

Security Requirements
(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).
(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.

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.
(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.
(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 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.
(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.
(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)".

Annex B (informative): H.248 Security

B.1 Background

To date, there has been an assumption that an operator's network represents a single trusted security domain, and therefore any communications that remain within that network are automatically trusted. A typical example of such an assumption is made in clause 4.5.1 of ES 283 002 [i.6].

In this architecture, it is assumed that everything within the dotted box in the associated diagram is part of the operator's domain. This assumption is then used to state that there is no need for any security mechanisms to be used to protect the communications between the AGW and the control subsystem or the RGW and the control subsystem in this case.

B.2 Challenging the assumption

In building an NGN, we have found cause to challenge this assumption. The reality of NGNs leads to believe that we can no longer trust the internal network, for several reasons:

- How can the operator, in a competitive, commercial world, enforce the residential gateway to be part of its domain? The reality will be that many different gateways with widely varying functionality will be used by customers.
- Operators are building network based on virtualized access gateways to allow for easy unbundling of customer lines. In such cases, although an unbundled customer will be physically attached to the operator's network, though logically they will be part of the unbundled operator's domain, connected via a virtualized access gateway. To make calls, signalling to and from the unbundled operator's core network is required.
- The lack of a secured signalling protocol will mean that specialist services such as LI will be less trustworthy when implemented on NGNs, compared to the present situation.
- For reasons of reduced costs and increased flexibility, NGNs are being built on IP transport networks, which are open and very well understood by potential attackers, compared to traditional, SS7 based telecommunications networks, which can be thought of as closed domains.
- IPsec has been accepted as the standard way of protecting IP based NGN interconnections (in the UK, by virtue of various NICC standards). The NICC IPsec profile is more complex than is proposed here, as it includes confidentiality protection using encryption in conjunction with integrity protection.
- Additionally, within the lifetime of current NGNs, it is certain that small operators (and possibly even some larger ones too) will leverage the Internet as their IP backbone for their NGNs.

For all these reasons, then, there is now a need for authentication of the communicating devices, and also a need to ensure that the signals they send or receive have not been tampered with en route.

The example given above relates to H.248 control signalling. Part of the H.248 standard defines a set of security requirements for signalling connections that are based around the well-known IPsec security standards from the IETF. IPsec is capable of using encryption and integrity security services, but it is proposed that only integrity protection is really needed.

The use of IPsec protected H.248 requires that the communicating entities are strongly authenticated to each other prior to communication. Also, it is necessary to renew the session keys used to protect the signalling data in transit at regular intervals. Unfortunately, the authors of the H.248 standard left these two important aspects out of their specifications, making do purely with a recommendation that the implementer of H.248 security make use of the IKE protocol for managing the connection, and X.509 certificates for authentication.

The lack of firm guidance on the management of IPsec connections within the H.248 standards has led to a variety of solutions to this problem being produced by equipment vendors, not all of which are compatible with IKE or indeed any other IPsec management solution. The net result is, of course, that for an operator striving to build an NGN by sourcing equipment from multiple vendors is that the use of IPsec to secure H.248 connections between multiple vendors' equipment becomes extremely difficult, if not impossible to manage using two or more mutually incompatible management mechanisms.

There would appear to be a couple of possible ways of building IPsec integrity protection into H.248:

- Requirements for such protection could be formulated and brought to the attention of the owners of the H.248 standard. This would be with the intention of defining a standard IPsec profile for protection of H.248, filling in the gaps in the present version of the standard.

- Requirements for such protection could be formulated within TISPAN and proposed as additions to the present document leading to normative text for Security for H248 (Release 2) 7.1 R-MGF Context and 7.2A-MGF Context in TS 187 005 [i.7] the Release 2 Security Architecture.

In either case, the requirements would have to encompass a standardized IPsec management solution. There are two possibilities:

- A solution according to TS 133 210 [3] and TS 133 310 [i.8]. However, it would have to be recognized that the certificate management would have to scale from a scheme being used within an operators domain and between a small number of operators with a pre-existing roaming agreements, to a scheme for a very large number of RGWs.

- A solution more suited to a large number of RGWs based on EAP-AKA and network certificates as specified in TS 133 234 [i.9] (WLAN 3GPP IP Access).

B.3 Possible disadvantages

IPsec is hard to configure - it adds an extra set of opportunities for problems when building a network. Using a standard IPsec profile is one way of minimizing this potential problem.

The use of IPsec to secure H.248 within an operator's network will require some development of any extant signalling monitors, such that they become capable of examining the payloads of IPsec authenticated packets. Currently, such monitors sit in the network and passively monitor signalling traffic that passes. This requirement does not imply that signalling monitors have to become part of the IPsec network, because the payload of an IPsec integrity protected packet is in the clear. No knowledge of the IPsec integrity protection key is required to be able to decode the signalling packet payload.

In the past, many equipment vendors and their customers have shied away from using IPsec on the grounds that it will adversely affect the performance of their devices. This is no longer really valid for modern computing hardware, where it is perfectly possible for devices such as mobile handsets to implement a fully automated IPsec solution without any problems such as extra delay.

Annex C (informative): Trust domains in NGN

NOTE: The term "trust" is not defined in ISO 27000 [i.10], "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

C.1 Definition of trust for the NGN - analysis

ISO 15408-1 does not directly define trust but does define a trusted channel and a trusted path. ISO 15408-2 defines functional capabilities (used in the functional requirement layer of the TISPAN Security requirements method in TR 187 011 [i.11]) 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.12] 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.

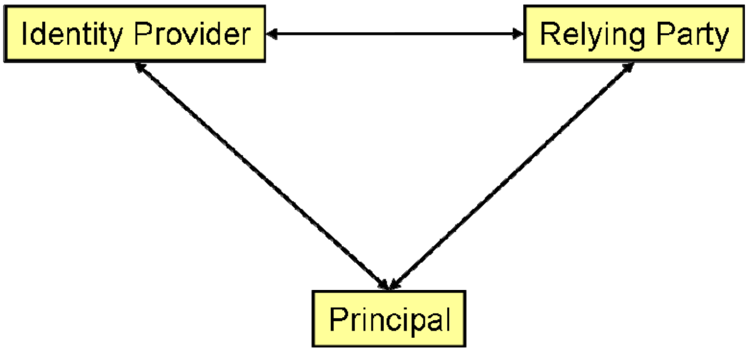

Figure C.1: Roles (or entities) in Authentication, SSO and Identity Federation scenarios (from TR 187 010)

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.

History

Document history		
V2.1.5	October 2008	Publication