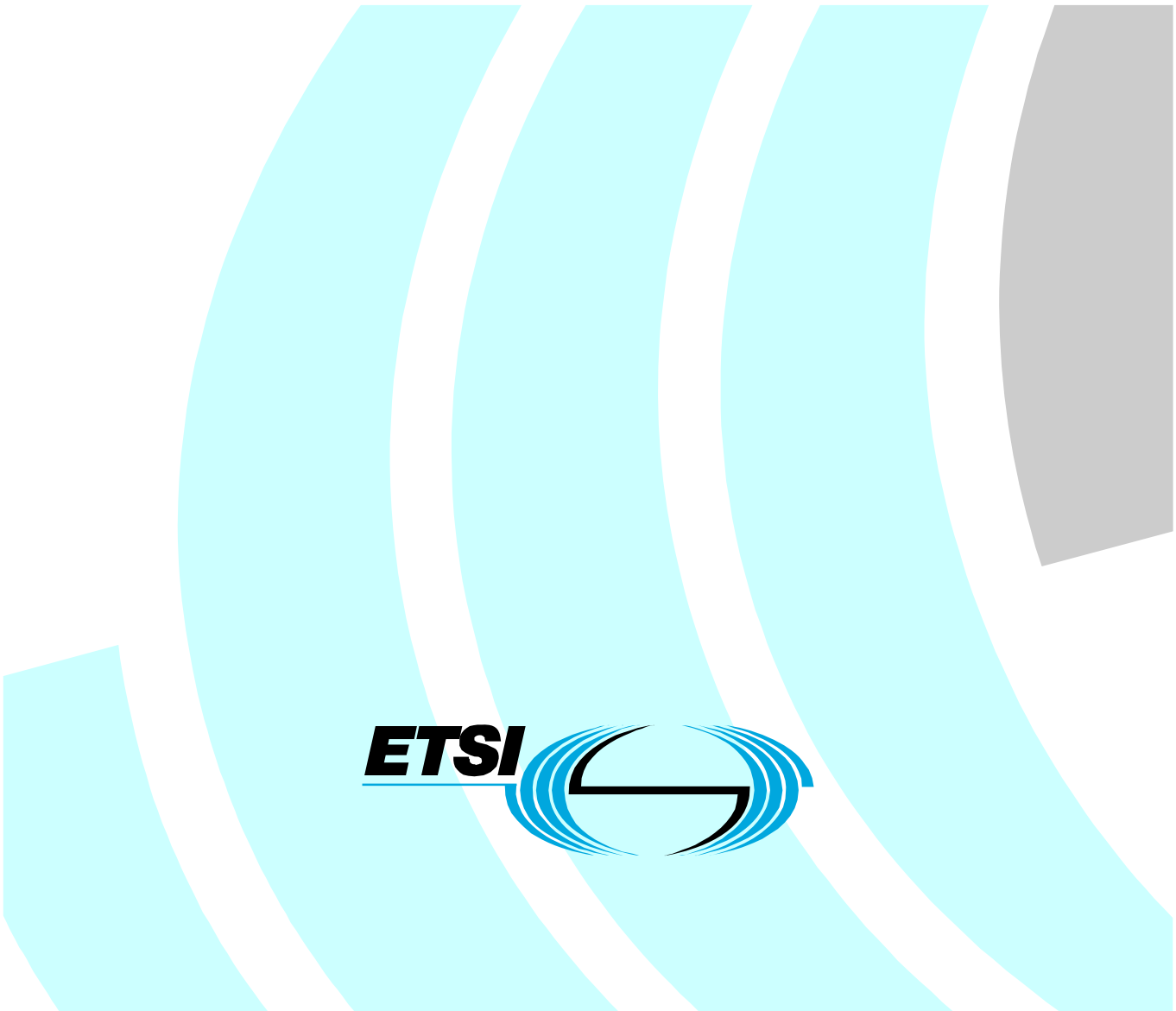
ETSI TS 187 016 V3.1.1 (2010-06)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)



Reference
DTS/TISPAN-07035-NGN-R3

Keywords
ID, security

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).

1 Scope

The present document specifies countermeasures to assure that users of the NGN have protection from abuse of identity. This covers authenticity and integrity countermeasures, including use of existing systems, and credential management in support of identity protection.

The present document:

- identifies the security objectives;
- defines the functional requirements (including those from ISO/IEC 15408-2 [i.6] that apply);
- defines the detail requirements for protection of identity in the NGN.

In doing so the present document:

- defines measures that provide protection of the NGN user identity from malicious traffic analysis;
- identifies those measures that allow compliance with the privacy legislation in the regions where the NGN is to be deployed where such legislation is known and public;
- identifies in Annex B a number of countermeasures in the form of policies or procedures.

The present document follows the recommendations of ES 202 382 [2] and provides an IdM PP Proforma which may be used as a basis for developing a PP for identity protection in an NGN subsystem deployment. The identity protection PP proforma is provided in Annex A.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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

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

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables". .

[2] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles ".

[3] ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

NOTE: Also available as ISO/IEC 9594-8.

[4] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[5] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[6] European Union Council Resolution COM 96/C329/01 of 17 January 1995 on the Lawful Interception of Telecommunications.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[8] ETSI TS 184 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Identifiers (IDs) for NGN". .

[9] ETSI TS 184 009: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Rules covering the use of TV URIs for the Identification of Television Channels".

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

[11] IETF RFC 5636: "Traceable Anonymous Certificate".

[12] OASIS Security Services: "Security Assertion Markup Language (SAML) v2.0".

2.2 Informative references

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

[i.1] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.2] UK Home Office, R.V.Clark: "Hot Products: understanding, anticipating and reducing demand for stolen goods", ISBN 1-84082-278-3.

[i.3] ISO/IEC 17799 (2005): "Information technology - Security techniques - Code of practice for information security management".

[i.4] ISO/IEC 13335: "Information technology - Security techniques - Guidelines for the management of IT security".

NOTE: ISO/IEC 13335 is a multipart publication and the reference above is used to refer to the series.

[i.5] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.6] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.7] AS/NZS 4360: "Risk Management".

[i.8] United Nations General Assembly resolution 217 A (III) 10 December 1948: "Universal Declaration of Human Rights".

[i.9] ITU-T Recommendation X.200: "Information technology - Open Systems Interconnection - Basic Reference Model: The basic model".

NOTE: Also available as ISO/IEC IS 7498-1.

[i.10] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[i.11] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis".

[i.12] Council of Europe European Treaties ETS No. 5: "Convention For Protection Of Human Rights And Fundamental Freedoms Rome, 4.XI.1950 ".

[i.13] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".

[i.14] ISO/IEC 10181-6: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework".

[i.15] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Access security for IP-based services (3GPP TS 33.203 version 8.6.0 Release 8)".

[i.16] ETSI TS 131 103: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the IP Multimedia Services Identity Module (ISIM) application (3GPP TS 31.103)".".

[i.17] ETSI TS 133 102: "Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture (3GPP TS 33.102)".

[i.18] IETF RFC 3323: "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[i.19] 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.20] ETSI TS 133 210: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 8.3.0 Release 8)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 387 [11], ISO/IEC 17799 [i.3], ISO/IEC 13335-1 [i.4] and the following apply:

asset: anything that has value to the organization, its business operations and its continuity

authentication: ensuring that the identity of a subject or resource is the one claimed

availability: property of being accessible and usable on demand by an authorized entity (ISO/IEC 13335-1 [i.4])

call: connection established by means of a publicly available telephone service allowing two-way communication in real time (Directive 2002/58/EC [4])

communication: any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communication service

NOTE: This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information (Directive 2002/58/EC [4]).

Concealable, Removable, Available, Valuable, Enjoyable, and Disposable (CRAVED): classification scheme to determine the likelihood that a particular type of item will be the subject of theft [i.2]

confidentiality: ensuring that information is accessible only to those authorized to have access

consent (by a user or subscriber)**:** correspond to the data subject's consent in Directive 95/46/EC [7] (Directive 2002/58/EC [4])

identifier: unique series of digits, letters and/or symbols assigned to a subscriber, user, network element, function or network entity providing services/applications

identity: set of properties (including identifiers and capabilities) of an entity that distinguishes it from other entities

identity crime: generic term for identity theft, creating a false identity or committing identity fraud

identity fraud: use of an identity normally associated to another person to support unlawful activity

identity theft: the acquisition of sufficient information about an identity to facilitate identity fraud

identity tree: the structured group of identifiers, pseudonyms and addresses associated with a particular user's identity

impact: result of an information security incident caused by a threat and which affects assets

information security incident: event which is the result of access to either stored or transmitted data by persons or applications unauthorized to access the data

integrity: safeguarding the accuracy and completeness of information and processing methods

location data: any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communication service (Directive 2002/58/EC [4])

mitigation: limitation of the negative consequences of a particular event

nonce: arbitrary number that is generated for security purposes (such as an initialization vector) that is used only one time in any security session

non-repudiation: ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

residual risk: risk remaining after countermeasures have been implemented to reduce the risk associated with a particular threat

risk: potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the attacked system or organization

subscriber: entity (associated with one or more users) that is engaged in a subscription with a service provider (refer to TS 184 002 [8])

subscription: commercial relationship between the subscriber and the service provider (refer to TS 184 002 [8])

threat: potential cause of an incident that may result in harm to a system or organization

NOTE 1: A threat comprises an asset, a threat agent and an adverse action of that threat agent on that asset (reference [i.5]).

NOTE 2: A threat is enacted by a threat agent and may lead to an unwanted incident breaking certain pre-defined security objectives.

threat agent: entity that can adversely act on an asset

traffic data: any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof (Directive 2002/58/EC [4])

unwanted incident: incident such as the loss of confidentiality, integrity and/or availability (ITU-T Recommendation X.200 [i.9])

user: any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service (Directive 2002/58/EC [4])

value added service: any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof (Directive 2002/58/EC [4])

vulnerability: weakness of an asset or group of assets that can be exploited by one or more threats

NOTE: As defined in ISO/IEC 13335 [i.4], a vulnerability is modelled as the combination of a weakness that can be exploited by one or more threats.

3.2 Abbreviations

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

AA	Attribute Authority
AC	Attribute Certificate
AKA	Authentication and Key Agreement
AMI	Authority Management Infrastructure
AS	authentication server
CA	Certificate Authority
CK	Cipher Key
CRAVED	Concealable, Removable, Available, Valuable, Enjoyable, and Disposable
CSCF	Call Session Control Function
CSP	Communications Service Provider
DAC	Discretionary Access Control
DNS	Domain Name Service
DoS	Denial of Service
ECN	Electronic Communications Network
ECN&S	Electronic Communications Networks & Services
ECS	Electronic Communications Service
GAA	Generic Authentication Architecture
HN	Home Network
HSS	Home Subscriber Server
IdM	Identity Management
IK	Integrity Key
IMEI	International Mobile Equipment Identity
IMS	Internet protocol Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
MAC	Mandatory Access Control
NAF	Network Application Function
NAI	Network Access Identifier
NASS	Network Access Sub-System
NDS	Network Domain Security
NGN	Next Generation Network
OASIS	Organization for the Advancement of Structured Information Standards
P-CSCF	Proxy CSCF
PES	PSTN Emulation Subsystem
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMI	Privilege Management Infrastructure
RA	Registered Area
RACS	Resource and Admission Control Subsystem
RBAC	Role Based Access Control
SAML	Security Assertion Markup Language
Sas	Security Associations
SIP	Session Initiation Protocol
SoA	Source of Authority
SpoA	Service point of Attachment
SSO	Single Sign-On
SuM	Subscription Management
TOE	Target Of Evaluation
TSF	TOE Security Function
TVRA	Threat Vulnerability and Risk Analysis
UA	User Agent
UE	User Equipment
UPM	User Profile Management

XML Extensible Markup Language

4 Identity and privacy protection in the NGN

4.1 Identity and privacy in the NGN

TR 187 010 [i.19] identifies a number of identity-related issues within the NGN, a set of security functional requirements and a set of measures that should be applied to counter the threats determined to exist in the NGN. The present document identifies a range of specific countermeasures to address threats to the management of identities within the NGN (including those arising from features added in NGN-R3) and specifies requirements necessary for complying with regulations on privacy [4], [7] as they apply to the NGN.

4.2 Regulatory requirements for privacy

The NGN should ensure consistency with Article 12 of the Universal Declaration of Human Rights [i.8] which states that "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*". This article is embodied in the EC directives on privacy (2002/58/EC [4]) and on data protection (EU Directive 95/46/EC [7]) with exceptions consistent with protection under law given by the directive on data retention (2006/24/EC [5]) and by the provisions for lawful interception given in COM 96/C 329/01 [6]. A detailed analysis of the impact of these regulations on the NGN can be found in clause 5.

The NGN is mandated by regulation to provide basic identity and privacy protection which introduces the following objectives to the NGN:

- the identity of an NGN user should not be compromised by any action of the NGN;
- no action of the NGN should make an NGN user liable to be the target of identity crime;
- the privacy of an NGN user should not be compromised by any action of the NGN; and
- the correspondence of an NGN user should not be compromised by any action of the NGN.

4.3 Behaviour and identity

Although an NGN user will have only one true identity, that user will be represented by multiple NGN identifiers which may be used to distinguish between the use of different services and capabilities. In addition, different identifiers will be associated with an NGN user at each different protocol layer.

However, this structure could expose behavioural and personal information and so the NGN needs to protect such information and prevent any unauthorized parties from linking behaviour to a specific NGN user. Figure 1 illustrates the link between a natural person and that person's behaviour and how that behaviour may act to identify the person. The communications behaviour of an NGN user is likely to be visible at several points in the network and an observer may be able to identify the user from an analysis of that behaviour.

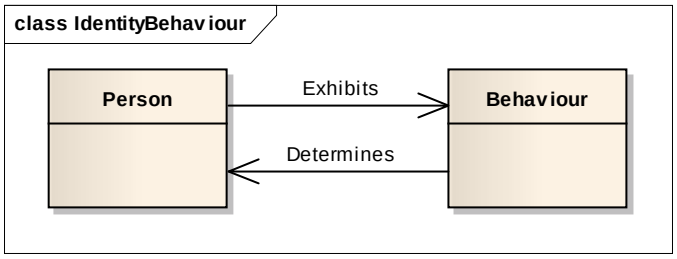


Figure 1: Link between person and behaviour

4.4 Identity protection objectives

Table 1 summarizes the security objectives related to Identity Management (IdM) in the NGN which were identified in TR 187 010 [i.19]. Objectives 7, 8, 9, 10 and 11 are included in Table 1 as a result of considering NGN Release 3 functionality and the European regulations on privacy and data protection.

Table 1: Security objectives related to IdM in the NGN

Objective	Statement
1	Access to NGN services should only be granted to users with appropriate authorization
2	The identity of an NGN user should not be compromised by any action of the NGN
3	No action of the NGN should make an NGN user liable to be the target of identity crime
4	No change in the ownership, responsibility, content or collection of personal data pertaining to an NGN user should occur without that user's consent or knowledge
5	Personal data pertaining to an NGN user should be collected by the NGN using legitimate means only
6	An audit trail of all transactions having an impact on personal data pertaining to NGN users should be maintained within the NGN
7	The identity of an NGN user should not be compromised by any action of the NGN
8	No action of the NGN should make an NGN user liable to be the target of identity crime
9	The NGN shall comply with the European regulations on privacy (EC Directives 2002/58/EC [4] and 2006/24/EC [5])
10	The NGN shall comply with the European regulations on data protection (EC Directive 95/46/EC [7])
11	The NGN shall comply with the requirements to support law enforcement (EC Directive 2006/24/EC [5]) and COM 96/C 329/01 [6])

4.5 NGN identity and identifiers

4.5.1 Identifying NGN users

In an ideal system there would be one unique NGN identity mapped to each NGN user. However, in practice an NGN identity comprises a number of NGN identifiers, each of which may be specific to a particular NGN sub-system, entity, application or protocol.

Identification, authentication and authorization are necessary both for billing purposes and for the tailoring of NGN services to an individual subscriber. An NGN user identifies itself to the NGN using an identifier that is recognised by the NGN but does not explicitly reveal the user's true identity. The NGN is able to map this identifier to the specific user although the many sub-systems of the NGN result in multiple representations of each user. In addition, user equipment and the NGN sub-systems themselves are required to be uniquely identifiable for the purposes of billing, error recovery, privacy, data retention and lawful interception.

4.5.2 Identifier attributes for identity protection

Table 2 lists a range of attributes which characterize each NGN identifier and which are the basis of identity management and protection within the NGN.

Table 2: NGN identifier attributes

Source of authority	The authority responsible for the provision of the identifier. Sources of authority include the CSP, a national regulatory authority and the NGN user (self asserted)
Purpose	The role of the identifier in the NGN (e.g. for registration, for call processing)
Persistence	The lifetime of the identifier
Resolution mechanism	The means by which the identifier is resolved to a network location

4.5.3 User Identifiers for non-communication services

For each NGN user there is at least one identifier which is assigned by the home operator and which is used both to identify the user's subscription and for non-communication services such as registration, authentication and mobility management. The attributes of such identifiers are listed in Table 3.

Table 3: Attributes of user identifier used for non-communication services

Source of authority	Home operator.
Purpose	Support of the authentication procedure during registration, de-registration, authorization, administration and accounting processes at the home IMS. Identification of the user within a dialog between network entities (e.g. UPSF or S-CSCF selection).
Persistence	Not tied to a particular call instance or session. Generally unchanged during the service lifetime of the user.
Resolution mechanism	Using the registration protocol (e.g. HSS/VSS).

4.5.4 User Identifiers for communication services

For each NGN user there is at least one identifier which is used for user-to-user communication within one or many services. The attributes of such identifiers are listed in Table 4.

Table 4: Attributes of user identifiers used for communication services

Source of authority	Service operator
Purpose	User to user communication to identify users to each other
Persistence	Not tied to a particular call instance or session. Generally unchanged during the lifetime of the user's subscription
Resolution mechanism	Generic mechanisms within the network (DNS, ENUM, routing tables)

4.5.5 Device Identifiers

Each device attached to the NGN has at least one fixed identifier which is used for associating the device user with a specific attachment point within the network. The attributes of such identifiers are listed in Table 5.

Table 5: Attributes of NGN device identifiers

Source of authority	Device manufacturer
Purpose	Binding a user to a physical network location
Persistence	Immutable. Fixed at manufacture and not modifiable through the lifetime of the device
Resolution mechanism	Network specific

4.5.6 NGN Service Identifiers

Each NGN service has at least one identifier which is used to distinguish it from any other service. The attributes of such identifiers are listed in Table 6.

Table 6: Attributes of NGN service identifiers

Source of authority	Service provider
Purpose	Provides an address with which subscribers can invoke the service
Persistence	Fixed, generally for the lifetime of the service but can be modified by the service provider if necessary
Resolution mechanism	Generic mechanisms within the network (DNS, ENUM, routing tables)

4.5.7 Network entity Identifiers within the NGN

Each network entity within the NGN has at least one identifier which distinguishes it from any other network entity.

NOTE: A network entity within the NGN is distinct from equipment. Several (logical) network entities may be supported by a single device.

The attributes of network entity identifiers are listed in Table 7.

Table 7: Attributes of network entity identifiers within the NGN

Source of authority	Network operator
Purpose	Provides an address which can be used by NGN services to gain access to the resources provided by the network entity
Persistence	Fixed, generally for the lifetime of the network entity but can be modified by the network operator if necessary
Resolution mechanism	Generic mechanisms within the network (DNS, ENUM, routing tables)

5 Analysis of regulatory requirements

5.1 Identification of personal data in the NGN

Directive 95/46/EC (Data protection Directive) [7] specifies the need for protection of individuals with regard to the processing of personal data and on the free movement of such data. Protection measures need to be provided within the NGN to ensure the rights and freedom of natural persons with regard to the processing of personal data and, in particular, their right to privacy.

Article 2a of the data protection directive [7] defines personal data as "*any information relating to an identified or identifiable natural person (data subject)*" where an identifiable person is "*one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". The definition is intentionally very broad and is intended to include data that, when processed by an attacker, may reveal the identity of a person or persons even if those persons are unable to make such a link themselves. Attacks of this type are generally referred to as "traffic analysis" attacks.

NGN identifiers can be used by both legitimate and illicit users to presume the identity of a person and, thus, are considered to be personal data. In some instances analysis of the behaviour of an NGN user may reveal further information that should be classified as sensitive personal data (e.g. religious beliefs, political opinions, health, sexual orientation and race). This may be implied by, for example, the connections between NGN users (e.g. phone calls, location of the user when invoking or receiving a service) or the source and content of services accessed by the NGN user using the NGN.

NOTE: Whilst private data may be found in the contents of a message exchange, the NGN should not have access to such data without resorting to forms of data inspection that may violate the requirement to protect the privacy of user data.

5.2 Privacy requirements

Directive 2002/58/EC [4] of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) requires that the confidentiality of private information in communication and the related traffic data is ensured. This includes communication over public communication networks and communication related to publicly available electronic communication services, i.e. the NGN. Consequently, the Directive requires the NGN to provide means of prohibiting the listening, tapping, storage and any other kind of interception and surveillance of communication and the related traffic data by persons other than users, without the consent of the concerned users except when legally authorised to do so.

The Directive also states that location data (other than traffic data) relating to users or subscribers of the NGN may only be processed when such data are made anonymous or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

5.2.1 Privacy exceptions required by regulation

The data retention directive 2006/24/EC [5] provides a legislative framework for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. The data retention directive itself refers to the exception to the Convention for the Protection of Human Rights and Fundamental Freedoms [i.12] which amends the text of the Universal Declaration on Human Rights to state in Article 8:

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

6 Identity protection functional requirements

6.1 Summary of security functional requirements

Table 8 lists the identity protection functional requirements refined from the identity protection security objectives in Table 1. A functional class (as defined in ISO/IEC 15408-2 [i.6]) is identified for each requirement and this is used in the development of functional security requirements for the NGN.

Table 8: Identity protection functional requirements

Functional requirement		Functional class
1	**Access to NGN services should only be granted to users with appropriate authorization**	
1.1	An NGN operator shall be the only entity able to create the identifiers in class 2	Access control policy
1.2	An NGN operator shall be the only entity able to destroy identifiers in class 2	Access control policy
1.3	An NGN shall support the secure transfer of identifiers and identities between CSPs	Export to outside TSF control
1.4	An NGN shall be able to enforce the use of NGN provided secrets for authentication	Specification of secrets
2	**The identity of an NGN user should not be compromised by any action of the NGN**	
2.1	An NGN shall protect the identities of its users from illicit misuse and abuse	Confidentiality
2.2	The identity of the identity provider should not be retrievable from analysis of a class 2 identifier	Unlinkability
2.3	An NGN operator shall endeavour to keep personal data accurate and up to date within the scope necessary for the achievement of the purposes of use	Data integrity
2.4	Personal data shall be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data	Access control policy; Stored data integrity; Export to outside TSF control
2.4.1	The NGN shall provide the capability to verify the integrity of all identity or identity revealing data transmitted between the NGN and the user terminal and perform deletion and notification if modifications are detected	Data integrity
2.4.2	The NGN shall provide the capability to correct transmission errors of all identity or identity revealing data transmitted between the NGN and the user terminal	Data integrity
2.4.3	The NGN shall protect identity or identity revealing data from modification when it is transmitted between separate parts of the NGN	Data integrity

Functional requirement		Functional class
2.4.4	The NGN shall be able to detect modification of identity or identity revealing data transmitted between separate parts of the NGN	Data integrity
2.4.5	The NGN shall be able to detect substitution of identity or identity revealing data transmitted between separate parts of the NGN	Data integrity
2.4.6	The NGN shall be able to detect re-ordering of identity or identity revealing data transmitted between separate parts of the NGN	Data integrity
2.4.7	The NGN shall be able to detect deletion of identity or identity revealing data transmitted between separate parts of the NGN.	Data integrity
2.4.8	Upon detection of an integrity error in identity or identity revealing data, the NGN shall delete the modified data and notify the receiving party	Data integrity
2.5	The NGN shall detect use of authentication data that has been forged by any user of the NGN	User authentication
2.6	The NGN shall detect use of authentication data that has been copied from any other user of the NGN	User authentication
2.7	The NGN shall provide a cryptographic symmetric challenge response mechanism to support user authentication	User authentication
2.8	The NGN shall provide a cryptographic asymmetric digest mechanism to support user authentication	User authentication
2.9	The NGN shall ensure that any third party is unable to determine whether any visible NGN transactions were caused by the same NGN user	Privacy; Unlinkability
2.10	The NGN shall ensure that any third party is unable to determine the real user name bound to the NGN identity	Privacy; Pseudonymity
3	**No action of the NGN should make an NGN user liable to be the target of identity crime**	
3.1	An NGN operator should provide the means for users to transact anonymously	Anonymity
3.2	NGN operators shall take reasonable measures to avoid collecting data capable of identifying an individual by referring to a database, in cases where such a possibility exists	Access control policy
3.3	The NGN shall prevent use of authentication data that has been forged by any user of the NGN	User authentication
3.4	The NGN shall prevent use of authentication data that has been copied from any other user of the NGN	User authentication
4	**No change in the ownership, responsibility, content or collection of personal data pertaining to an NGN user should occur without that user's consent or knowledge**	
4.1	An NGN operator should obtain the prior and unambiguous consent of the data subject for the collection of personal data and indicate the purposes of use before collecting personal data	Access control policy
4.2	An NGN operator shall inform the data subject of the collection of personal data and the indicated purposes of use before collecting personal data	Access control policy
4.3	When handling personal data, an NGN operator shall specify the purposes of use of personal data	Access control policy
4.4	An NGN operator should not change the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes	Access control policy
4.5	Before an NGN operator changes the purposes of use beyond the scope in which new purposes can reasonably be considered to be compatible with the original purposes, it should inform a data subject of the change or obtain prior and unambiguous consent	Access control policy
4.6	An NGN operator should not handle personal data, without obtaining the prior consent of the data subject, beyond the scope necessary for the achievement of the specified purposes of use	Access control policy
4.7	An NGN operator should not provide personal data to a third party without obtaining the prior consent of the data subject.	Export to outside TSF control
4.8	There should be a general policy of openness about developments, practices and policies with respect to personal data	Access control policy

	Functional requirement	Functional class
5	**Personal data pertaining to an NGN user should be collected by the NGN using legitimate means only**	
5.1	An NGN operator shall not acquire personal data by fraudulent or other dishonest means	Information flow control policy
6	**An audit trail of all transactions having an impact on personal data pertaining to NGN users should be maintained within the NGN**	
6.1	The NGN operator shall maintain an audit log of all class 2 identifiers created and destroyed	Security audit event storage
6.2	The NGN CSP shall maintain an audit log of all user identities transferred to or from another CSP	Security audit event storage
6.3	The NGN operator shall maintain an audit log of all requests for consent for the collection of personal data and the responses received from the data subject	Security audit event storage
6.4	The NGN operator shall maintain an audit log of all instances where it has informed the data subject of the collection of personal data	Security audit event storage
6.5	Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data collector	Security audit data generation
6.6	Audit records shall be viewable only by authorized parties	Access control policy
6.7	The NGN shall be able to associate each auditable event with the identity of the user that caused the event	Security audit data generation
7	**The identity of an NGN user should not be compromised by any action of the NGN**	
7.1	The NGN shall ensure that no third party is able to determine whether any visible NGN transactions were caused by the same NGN user	Unlinkability
7.2	The integrity of an identity and any identity-revealing data should be assured when it is transferred within the NGN	Integrity of transmitted data
8	**No action of the NGN should make an NGN user liable to be the target of identity crime**	
8.1	The confidentiality of identities, identity revealing information, private information and data that can be used to relate behaviour to identity shall be ensured when transferred within the NGN	Confidentiality of transmitted data
9	**The NGN shall comply with the European regulations on privacy (EC Directives 2002/58/EC [4] and 2006/24/EC [5])**	
9.1	The NGN shall ensure that no third party is able to determine the real user name bound to an NGN identity	Pseudonymity
10	**The NGN shall comply with the European regulations on data protection (EC Directive 95/46/EC [7]**	
10.1	The NGN shall ensure that only authorized parties are able to access any information binding an NGN identifier to the true identity of a user	Authenticity

6.2 Security capabilities required in the NGN for identity protection

6.2.1 Access control measures

6.2.1.1 Authenticity

Establishing the access rights of an NGN user involves three distinct but related capabilities, as follows:

1) Identification

   - the assertion of an NGN user's identity in order to gain access to NGN services. This involves the use of pseudonyms and other identifiers;

2) Authentication

   - the validation of the identity of either an NGN user or the NGN itself. A user's identity can be validated using weak authentication methods such as username and password or strong authentication based on cryptographic procedures;

3) Authorization

- the assertion and verification of an NGN users permission to invoke specific NGN services or gain access to sensitive internal data.

These capabilities are all significant aspects of IdM within the NGN but it is the Authorization component which is of particular importance to the protection of a user's privacy as it is used to establish and control the right to access the data linking users' various pseudonyms and their true identities.

6.2.2 Privacy measures

6.2.2.1 Pseudonymity

Pseudonymity ensures that a user may use a resource or service without disclosing its user identity, but can still be held accountable for that use. A pseudonym is an identifier allocated by an NGN authority to a single entity or group of entities and which bears no relation to the true identity of the entity or group. In this way, it is only the NGN authority that is able to resolve a pseudonym to a true identity. By changing pseudonyms on a regular basis the real identity can also be protected from behavioural analysis attacks.

6.2.2.2 Unlinkability

Unlinkability ensures that a user may make multiple uses of resources or services without others being able to link these uses together. This means that within the NGN from the perspective of an unauthorized party, NGN users and their actions in the NGN are no more and no less related after an observation than they are related concerning the a-priori knowledge. Therefore, the probability of particular actions being related to particular NGN users remains the same after an observation as it was before.

The unlinkability of two (or more) messages may depend on whether their content is protected against a particular attacker. Messages may be considered to be unlinkable if the attacker is unable to acquire information on the sender or recipient of a message by analyzing the message. Nevertheless, even simple analysis of the contents of a number of messages can reveal certain characteristics which link them together - for example, similarities in structure and style, the use of particular words or phrases and the consistent use of specific grammatical errors.

Pseudonyms may serve as a basis for unlinkability but their use does not, on its own, guarantee that any link between users and their behaviour will be hidden from an attacker.

6.2.3 Confidentiality measures

The confidentiality of identities, identity revealing information, private information and data that can be used to relate behaviour to identity shall be ensured when transferred within the NGN. This is of particular importance for ensuring unlinkability.

6.2.4 Integrity measures

6.2.4.1 Transmitted data protection (integrity)

The integrity of identities and any identity-revealing data should be assured when it is transferred within the NGN. If there is any doubt about the integrity of received data which is required by an invoked service capability, that service capability should be terminated.

The NGN system shall provide integrity services classified by the criteria given in ISO/IEC 10181-6 [i.14], as follows:

1) By the type of violation they protect against. The types of violation are:

- unauthorized data modification;
- unauthorized data creation;
- unauthorized data deletion;
- unauthorized data insertion;

- unauthorized data replay.

2) By the type of protection they support. The types of protection are:

   - prevention of integrity compromise;

   - detection of integrity compromise.

3) By whether they include recovery mechanisms or not:

   - with recovery:

     - may be possible to recover the original data (and possibly signal a recovery action or an error for purposes such as audit) whenever the validation of received data indicates that an alteration has occurred;

   - without recovery:

     - it is unlikely to be possible to recover the original data whenever the validation of received data indicates that an alteration has occurred.

6.2.5 Credential management

The security capabilities described in clauses 6.2.1, 6.2.2, 6.2.3 and 6.2.4 use a number of cryptographic keys and other security credentials in order to be effective. The credential management capability provides assurance that these items are created, transmitted and stored securely without modification, interference or observation by unauthorized parties. These credentials are as follows:

I-AK	Infrastructure Identity Authentication Key
U-AK	User Identity Authentication Key
I-IK	Infrastructure Integrity Key
U-IK	User Integrity Key
IU-SCK	Infrastructure to User Session Confidentiality Key
IG-SCK	Infrastructure to Group Session Confidentiality Key
UI-SCK	User to Infrastructure Session Confidentiality Key

Table 9 identifies how each of the credentials is used within different types of security association.

Table 9: NGN security credentials

Origin	Destination	Authenticity	Integrity	Confidentiality	Association
User	User	I-AK, I-AK	I-IK, U-IK	UI-SCK, IU-SCK	Indirect (note 1)
User	User-Group	I-AK, U-AK	I-IK, U-IK	UI-SCK, IG-SCK	Indirect
NGN	User	U-AK	I-IK	I-CK	Direct (note 2)
NGN	User-Group	I-AK	I-IK	G-CK	Direct
User	NGN	U-AK	U-IK	UI-SCK	Direct
NOTE 1: An indirect association depends upon the separate direct associations between each terminating user and the NGN to imply the authentication, integrity and confidentiality parameters associated with the end-to-end session. NOTE 2: A direct association depends only on the authentication, integrity and confidentiality parameters specified for itself.					

6.2.6 Audit and accounting measures

The actions of the NGN user may be recorded for the purposes of accounting leading to billing. In addition the actions of the NGN user have to be recorded for Data Retention [5]. In each case the data recorded should be only visible to authorised entities and removed after consumption (or expiry in the case of data retained in accordance with the Data Retention directive).

7 Identity Protection Framework

7.1 PKI-based Framework elements

The NGN identity protection framework comprises three elements, as follows:

1) Public Key Infrastructure (PKI);

2) Public Key Certification Schema (PKC); and

3) Privileged Management Infrastructure (PMI).

Each is described in the following clauses.

7.2 Public Key Infrastructure (PKI)

A public key infrastructure (PKI) enables users of public networks to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The main elements of a public key infrastructure are a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. PKI assumes the use of public key cryptography for authenticating a message sender or for encrypting a message.

A public key infrastructure consists of:

- a certificate authority (CA) that issues and verifies digital certificates
  - a certificate includes the public key or information about the public key;
- a registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor;
- one or more directories where the certificates (with their public keys) are held; and
- a certificate management system.

Additionally, PKI requires an effective key distribution and management model which includes revocation capabilities that scale to the size of the network and the number of its communicating entities. As the authenticity of a message is established by verification of the certificate included by the message sender, the communicating parties need to be notified if and when certificates have been compromised or are, for other reasons, no longer valid. The revocation of certificates is challenging, particularly within the NGN where it might be necessary to operate with multiple authorities and sub domains offering a variety of communication services.

7.2.1 Public Key Certification (PKC)

A public key certificate (also known as a digital certificate or identity certificate) is an electronic document that uses a digital signature to bind together a public key with an identity. The information that defines the identity information of a person or organization includes:

- their name;
- their address;
- their location;
- any explicit identity revealing information; and
- any information that can be used to link specific behaviour to specific individuals.

A certificate is used to verify that a public key belongs to an individual. It is validated by the digital signature of an authoritative entity known to all communicating parties.

There are two types of PKC of relevance for NGN:

1) time-variant pseudonym certificate; and

2) anonymous certificates.

Both types of PKC include an authoritative identity which is traceable back to the real identity only by the CA.

7.2.1.1 Traceable time-variant pseudonym certificates with authoritative identity

Messages in the NGN may contain different identifiers at each layer of the protocol stack. Such identifiers may carry information that can be used to derive the real identity of the user or to link behaviour to specific NGN users, particularly at the application layer. Examples of such information include user's name, user's address, location and equipment identities. To prevent an eavesdropper from acquiring this personal information, the NGN uses a variety of identifiers across its sub-systems and services. Some of these identifiers can be looked upon as "pseudonyms" that are not directly linked to the user's true identity while others can be directly traced to specific NGN users.

The NGN needs to be able to trace traffic to a specific NGN user so that the user can be billed for the use of all non-anonymous subscription services. However, it is still necessary to protect users' identities and their right to privacy so no identity revealing information shall be transmitted and pseudonymity shall be ensured at all layers of the protocol stack.

Pseudonymity ensures that a user may have access to a resource or service without disclosing its true identity but can still be held accountable for that use. A pseudonym is an identifier allocated by an NGN authority to a single entity or group of entities and which bears no relation to the true identity of the entity or group. In this way, it is only the NGN authority that is able to resolve a pseudonym to a true identity. By changing pseudonyms on a regular basis the real identity can also be protected from behavioural analysis attacks.

The use of pseudonyms can only be considered effective if the method used is able to guarantee that:

- the user's true identity is hidden from all other users;
- the user's true identity cannot be derived from observation of that user's behaviour; and
- only authoritative entities can trace the pseudonym back to a real NGN user identity.

7.2.1.2 Traceable anonymous certificates with authoritative identity

The NGN may offer services that are free of charge or that, for other reasons, are not reliant upon the use of identity and identity revealing information for charging and billing. These services are referred to as anonymous services and require anonymous certificates which are defined in RFC 5636 [11].

NOTE: It is assumed that overall the NGN is a paid for facility but that some services may be provided without the need for explicit identification of the user (thus anonymous) and may include the receiving of broadcast services over the NGN (e.g. IPTV).

An anonymous certificate is one which contains no information related to the holder's true identity in the subject field. Anonymous certificates can be used to enhance user privacy. However, as an X.509 certificate must contain an identifier to comply with PKI format standards and a CA must not issue multiple certificates with the same Subject name to different entities, the level of privacy offered by anonymous certificates depends on the type and randomness of the identifiers used.

There is a need to balance privacy and accountability when issuing anonymous certificates for audit and other reasons. If a CA or RA is unable to resolve an anonymous certificate to the real user to whom it was issued, the user is able to abuse the anonymity afforded by the certificate because there would be no recourse for relying parties. An anonymous certificate should, therefore, be traceable by the CA or RA back to the user to whom it was issued. It is imperative that only authoritative entities are able to establish this link. This can be ensured if the authoritative entity initially identifies the user and maintains a database that relates the user's true identity to the random identifier carried in the certificate's Subject field.

7.2.2 Privilege Management Infrastructure (PMI)

A Privilege Management Infrastructure (PMI) is a cryptographic certificate-based approach to asserting the rights of a user or application to access or modify data or invoke services within a system. A PMI carries user privileges in the form of attributes in an Attribute Certificate (AC) which is issued to the user by either s Source of Authority (SOA) or an Attribute Authority (AA). PMIs rely on an underlying public key model because ACs need to be digitally signed by the issuing AA and because a network-wide, known, trusted and non-forgeable authoritative identity information must be used to validate the AA's signature.

Examples of PMIs are ITU-T Recommendation X.509 [3], Kerberos and the Security Assertion Markup Language (SAML).

7.2.2.1 ITU-T Recommendation X.509

ITU-T X.509 [3] privilege management. uses the attributes in an attribute certificates (ACs) to communicate, assert and validate user privileges. Access rights are held within the privilege attributes of Acs that are issued to users. Each privilege attribute describes one or more of the user's access rights. A target resource reads a received AC to validate that the originating user is authorized to perform the action that is being requested.

The SOA is the owner of the resource and is responsible for assigning privileges to other entities which are either Attribute Authorities if they can delegate their privileges further or privilege holders if they are not. An AA is permitted to delegate privileges to other entities (both AAs and privilege holders) but may or may not be able to assert the privileges itself. The privilege verifier is the entity that checks the asserted privileges and makes a yes/no decision as to whether the privilege may be used or not. The privilege verifier trusts the SOA and checks that the privilege holder has been directly or indirectly authorised by the SOA.

7.2.2.2 Kerberos

Kerberos is a ticket-based authorization system which provides a means of verifying the identities of the principals (e.g. an NGN user and a server) of a transaction in an open (unprotected) network. This is accomplished without relying on assertions by the host operating system, without basing trust on host addresses, without requiring physical security of all the hosts on the network and under the assumption that packets travelling through the network can be read, modified and manipulated at will. Kerberos authenticates a user be means of conventional (shared secret key) cryptography before granting the user authorization to access a remote server. Extensions to Kerberos can provide for the use of public key cryptography during certain phases of authentication.

The basic Kerberos authorization process proceeds as follows:

1) A client sends a request to the authentication server (AS) for "credentials" for a given server.

2) The AS responds with these credentials, encrypted in the client's key. The credentials consist of a "ticket" for the server and a temporary encryption key (often called a "session key").

3) The client transmits the ticket (which contains the client's identity and a copy of the session key, all encrypted in the server's key) to the server.

4) The session key (now shared by the client and server) is used to authenticate the client and may optionally be used to authenticate the server. It may also be used to encrypt further communication between the two parties or to exchange a separate sub-session key to be used to encrypt further communication.

NOTE: Many applications use the functions of Kerberos only upon the initiation of a stream-based network connection. Unless an application performs encryption or integrity protection for the data stream, the identity verification applies only to the initiation of the connection, and it does not guarantee that subsequent messages on the connection originate from the same principal.

7.2.2.3 Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) [12] is an XML-based standard for exchanging authentication and authorization data between security domains, i.e. between an identity provider (a producer of assertions) and a service provider (a consumer of assertions).

SAML has been developed by the OASIS Security Services Technical Committee to provide Web Browser Single Sign-On (SSO) but has been extended to be an authorization mechanism that can be used for various types of network.

It assumes that the principal (the NGN user) has enrolled with at least one identity provider which is responsible for ensuring local authentication services to the principal. This means that the service providers in the network (those offering services to the users) rely on the identity provider for registration services. This registration results in what is called a SAML assertion which on the user's request is passed to the service provider. The service provider makes access control decisions based on the forwarded SAML assertions.

SAML is built upon a number of existing standards:

- Extensible Markup Language (XML):
  - most SAML exchanges are expressed in a standardized dialect of XML;
- XML Schema:
  - SAML assertions and protocols are specified (in part) using XML Schema;
- XML Signature:
  - digital signatures based on the XML Signature standard are used for authentication and message integrity;
- XML Encryption:
  - SAML 2.0 uses XML Encryption to provide elements for encrypted name identifiers, encrypted attributes, and encrypted assertions (SAML 1.1 does not have encryption capabilities);
- Hypertext Transfer Protocol (HTTP):
  - SAML relies on HTTP as its communications protocol;
- Simple Object Access Protocol (SOAP):
  - SAML specifies the use of SOAP 1.1.

SAML defines XML-based assertions and protocols, bindings, and profiles. The term SAML Core refers to the general syntax and semantics of SAML assertions as well as the protocol used to request and transmit those assertions from one system entity to another. SAML protocol refers to what is transmitted, not how (the latter is determined by the choice of binding).

7.2.2.4 Access control models in PMI

PMI supports all of the three traditional access control models:

- Discretionary Access Control (DAC);
- Mandatory Access Control (MAC); and
- Role Based Access Control (RBAC).

The scheme for verifying privileges is independent of the model used.

DAC leaves the granting and revoking of access privileges to the discretion of the individual user. A DAC mechanism allows users to grant or revoke access to any of the objects under their control without the intercession of an authority.

MAC enforces access controls on the basis of security labels which are attached to users (more precisely, to subjects) and objects and are controlled by a central authority. Users can only access objects assigned an equal or lower security label than their own. The underlying principle is to provide information to higher levels in the hierarchy (write-up) and access information from lower down in the hierarchy (read-down).

Access control decisions are often determined by the roles individual users take on as part of an organization. This includes the specification of duties, responsibilities and qualifications. For example, the roles of an individual NGN user can be associated with subscription groups, the way that the NGN is used or the way that the NGN bundles services such as IPTV to deliver to users. Role based access control (RBAC) enables access control decisions to be made based on the functions a user is authorized to perform within the NGN. Unlike DAC, the user cannot pass access permissions on to other users at their discretion.

7.3 Analysis of framework elements

This evaluation of potential NGN identity protection framework elements makes explicit the consequences of each element on the NGN architecture, sub-systems and services. Each element is evaluated in the context of the security capabilities needed to comply with the regulatory requirements identified in clause 5.

There are two implementation strategies specified for the NGN Identity Protection Framework elements based on the countermeasure strategies defined in TS 102 165-1 [i.1], as follows:

(i) asset redesign:

- removal of identified identity protection problem areas through fundamental design changes in the NGN architecture or affected NGN subsystems;
- can reduce both the likelihood and the overall impact of a successful attack.

(ii) asset hardening:

- specification of additional security capabilities and services to the NGN that will mask the effects of an identity protection problem area rather than remove it completely;
- likely to be used in cases where:
  - the cost of asset redesign is unacceptable;
  - the change itself is unnecessarily complex; or
  - redesign does not reduce the risk level to *Minor*;
- can only affect the likelihood of a successful attack, not the impact.

The costs involved with each of the framework elements are evaluated in terms of the following:

- impact on standards design:
  - No impact, Low impact, Medium impact and Major impact.
- impact on implementation costs:
  - No impact, Low impact, Medium impact and Major impact.
- impact on operation costs:
  - No impact, Low impact, Medium impact and Major impact.
- regulatory impact:
  - Severe negative impact, Negative impact, No impact, Positive impact, Significant positive impact.
- market acceptance:
  - Severe negative impact, Negative impact, No impact, Positive impact, Significant positive impact.

7.3.1 Public Key Infrastructure (PKI)

The costs of implementing an NGN-wide PKI or a hierarchical NGN PKI across multiple administrative domains are evaluated as follows:

Impact on standards design	-	Major
Impact on implementation	-	Major
Impact on Operation	-	Major
Regulatory impact	-	Positive
Market acceptance	-	Negative

- Implementation strategy:
  - Asset redesign.
- Advantages:
  - Enables verification of authenticity of messages.
  - Protects the confidentiality of message contents.
  - Public keys can be used to derive integrity keys for protecting the integrity of identity information.
  - Includes authoritative identity information (depending on the key management schema).
- Disadvantages:
  - Public keys include information about the key holder and therefore reveal identity relevant information.
  - Public key operations are slow relative to symmetric key operations and may not be feasibility for some NGN services.
  - Jurisdiction of CA may be complex - are they national / EU-wide / other?
  - Distributing revocation information may aspire DoS like circumstances reducing the resources available to NGN services.
  - Distributing revocation information may be complex as there are multiple administrative domains.
  - It involves additional administrative activities for the users.
- Implications on NGN Architecture, sub-systems and services:
  - Addition of a CA hierarchy across administrative domains that can effectively distribute and revoke keys.
  - Addition of a trust hierarchy between the Cas in the multi-domain CA hierarchy and procedures to continuously evaluate these trust relations.
  - Additions of entities in the NGN that can detect and act upon misuse of keys.
- Ability to address relevant regulatory requirements:
  - Addresses the regulatory requirement "Where data is transferred in the NGN and contains identity or identity revealing data the confidentiality of the transferred data should be assured".
  - Addresses the regulatory requirement "Where data is transferred in the NGN and contains identity or identity revealing data the integrity of the transferred data should be assured".

7.3.2 Public Key Certification

The costs of extending the NGN with a PKC mechanism are evaluated as follows:

Impact on standards design	-	Medium
Impact on implementation	-	Minor
Impact on Operation	-	Minor
Regulatory impact	-	Positive
Market acceptance	-	Negative

- Implementation strategy:
  - Asset hardening.
- Advantages:
  - Digital signatures can be used to derive confidentiality and integrity keys.

- Enables integrity of identity and identity-related information.
- Enables confidentiality of identity and identity-related information (pseudonyms).
- Public key of an authoritative entity represent an authoritative identity in a certificate and can be used to enable validation of the authenticity of messages.

- Disadvantages:
  - Certificate hierarchy may be complex as NGN involves multiple administrative domains.
  - Distributing revocation information may aspire DoS like circumstances reducing the resources available to NGN services.
  - Distributing revocation information may be complex as there are multiple administrative domains.
- Implications on NGN Architecture, sub-systems and services:
  - Addition of certificate hierarchy and procedure for continuously evaluating and managing trust relations within the hierarchy.
  - Addition of certification revocation services.
  - Additions of entities in the NGN that can detect and act upon misuse of certificates.
- Ability to address relevant regulatory requirements:
  - Addresses the regulatory requirement "Where data is transferred in the NGN and contains identity or identity revealing data the confidentiality of the transferred data should be assured".
  - Addresses the regulatory requirement "Where data is transferred in the NGN and contains identity or identity revealing data the integrity of the transferred data should be assured".
  - Addresses the regulatory requirement "The NGN shall ensure that any third party is unable to determine the real user name bound to the NGN identity".
  - Addresses the regulatory requirement "The NGN shall ensure that any third party is unable to determine whether any visible NGN transactions were caused by the same NGN user.

7.3.3 Privilege Management Infrastructure (PMI)

The costs of introducing PMI into the NGN are evaluated as follows:

Impact on standards design	-	Medium
Impact on implementation	-	Medium
Impact on Operation	-	Medium
Regulatory impact	-	Positive
Market acceptance	-	No impact

- Implementation strategy:
  - Asset redesign and asset hardening.
- Advantages:
  - PMI supports all three traditional access control models and can therefore easily extend existing authorization schemas.
  - Authorization does not need to include identity information traceable to individual users and can be based on e.g. subscription groups.
  - Allows multiple SoA and AA across administrative domains and easy transfer of rights to issue authorization tickets (AC).
  - Support symmetric and asymmetric keying and encryption.

- Disadvantages:
  - Adds a further level of key management to NGN.
  - Makes it more difficult for service providers to associate traffic or service usage to individual users.
- Implications on NGN Architecture, sub-systems and services:
  - Addition of an authoritative hierarchy across administrative domains to use for authorization in the NGN.
  - Addition of application layer security services to handle ACs and authorization requests.
  - Involve change to current charging routines (may add extra services to trace service usage to individual users or subscribers).
- Ability to address relevant regulatory requirements:
  - Addresses the regulatory requirement: "Only authorized parties can access services and the bindings of the identifiers of an NGN user".
  - Addresses the regulatory requirement "Where data is transferred in the NGN and contains identity or identity revealing data the confidentiality of the transferred data should be assured".
  - Addresses the regulatory requirement "Where data is transferred in the NGN and contains identity or identity revealing data the integrity of the transferred data should be assured".
  - Enables audit without revealing true identity or information that can be used to deduce the true identity.

7.3.4 Summary of analysis results and recommendations

The following list of observations summarizes the results of the analysis of the NGN Identity Protection Framework elements:

- Identity protection in the NGN requires a combination of registration, authentication and authorization:
  - registration must ensure that identity and identity-related information are not communicated in clear-text as part of authentication requests, authorization requests and service consumption.
- PMI provides all the necessary security capabilities except anonymity, pseudonymity and unlinkability within reasonable cost.
- PKC provides all the necessary security capabilities.
- PKI does not provide all the necessary security capabilities but includes relatively large implementation and operation costs and implies a major impact on standards design.

Therefore, the authentication and authorization model of identity protection in the NGN should be based on the core principles in PMI, extended with a registration and privacy mechanism based on PKC.

8 Identity management and protection within the NGN

8.1 NGN identifiers

TS 184 002 [8] provides a complete overview (dated October 2006) of the identifiers in the NGN and is supplemented by more recent work for IPTV that specifies the iptv:uri in TS 184 009 [9]. The current state identified in these documents is summarised in Table 10 and structured here against the ECN&S regulatory model.

Table 10: NGN identifiers

ECN&S layer	Abbreviation	Long form	OSI layer	Used as AKA principal
ECS	IMSI	International Mobile Subscriber Identity	7, used as registration name	Yes, UMTS-AKA
	MSISDN	Mobile Station international ISDN number	7, used as telephone number	
	SIP URI	SIP Universal Resource Identifier	Used in SIP Protocol	
	IMPU (as NAI)	IMS Public User Identity	Used in SIP (equivalent to MSISDN for 2G domain)	
	IMPI (as NAI)	IMS Private User Identity	Used in SIP REGISTER message to identify subscription	Yes, IMS-AKA
	E.164 ID	E.164 telephone number	7, used as name	
	Tel URI	Telephone URI	Used in SIP Protocol	
ECN	IP address	The IP address of the attached user equipment	Layer 3 (network)	
	Address realm	The addressing domain in which the IP address is significant	Layer 3	
	Physical Access ID	The identity of the physical access to which the user equipment is connected	Layer 1 and 2 (MAC address)	
	Logical Access ID	The identity of the logical access used by the attached user equipment. In the xDSL case, the Logical Access ID may explicitly contain the identity of the port, VP and/or VC carrying the traffic	Layer 2	
Not defined	Subscriber Id	The identity of the attached user	Not used for communication	
	IMEI	International Mobile Equipment Identity	Not used in communication	

8.2 Identity protection in SIP (current state)

The SIP protocol in RFC 3325 [10] offers two mechanisms for use in exchanging an asserted identity within trusted networks (a single trust domain). The mechanisms are not intended to offer a general privacy or identity model suitable for use between different trust domains and thus may not apply to the generic NGN where the NGN is modelled as a set of co-operating trust domains.

- p-asserted-identity:
  - The P-Asserted-Identity header is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication.
- p-preferred-identity.

8.2.1 SIP privacy handling in the NGN

Some support for SIP privacy handling in the NGN is described in TS 133 203 [i.15].

- SIP Privacy handling in IMS Networks:
  - Privacy may in many instances be equivalent with confidentiality i.e. to hide the information (using encryption and encryption keys) from all entities except those who are authorized to understand the information. The SIP Privacy Extensions for IMS Networks do not provide such confidentiality. The purpose of the mechanism is rather to give an IMS subscriber the possibility to withhold certain identity information of the subscriber as specified in RFC 3323 [i.18] and RFC 3325 [10].

NOTE: It is recommended that the privacy mechanism for IMS networks does not create states in the CSCFs other than the normal SIP states.

- SIP Privacy handling when interworking with non-IMS Networks:

  - When a Rel-6 IMS is interworking with a non-IMS network, the CSCF in the IMS network shall decide the trust relation with the other end. The other end is trusted when the security mechanism for the interworking (see clause 6.5) is applied as well as the availability of an inter-working agreement. If the interworking non-IMS network is not trusted, the privacy information shall be removed from the traffic towards to this non-IMS network. When receiving SIP signalling, the CSCF shall also verify if any privacy information is already contained. If the interworking non-IMS network is not trusted, the information shall be removed by the CSCF, and retained otherwise.

  - Because absence of the security mechanism for the interworking (see clause 6.5) indicates an untrusted non-IMS network, separate CSCFs are usually needed to interface with IMS and non-IMS networks. The CSCF interfacing with IMS networks implicitly trusts all IMS networks reachable via the SEG that establishes security according to TS 33.210 [i.20]. A Rel-5 CSCF always assumes this trust relationship and network configuration. For a Rel-6 CSCF, this implicit trust setting shall be a configuration option, that an operator can set according to his network and interface configuration.

8.3 Identity protection in IMS (IMS-AKA)

8.3.1 Overview

Identity protection in IMS is covered by authentication of the IMPI and by registration of IMPUs to the IMPI with any SIP messages containing identity revealing data protected by the allocation of an Ipsec tunnel between the UE and the edge of the IMS network.

8.3.2 IMS security analysis

As defined in TS 133 203 [i.15] a set of security associations between the multimedia client and the IMS is required before access is granted to multimedia services. The specification of IMS credentials and their management on a UICC is defined in TS 131 103 [i.16] whilst the algorithm set used by IMS-AKA is described in TS 133 102 [i.17].

NOTE 1: IMS AKA is only mandated when the IMS user accesses IMS through UMTS but is recommended (Annex L of TS 133 203 [i.15]) for when the transport domain is modelled as a Generic IP Transport stratum.

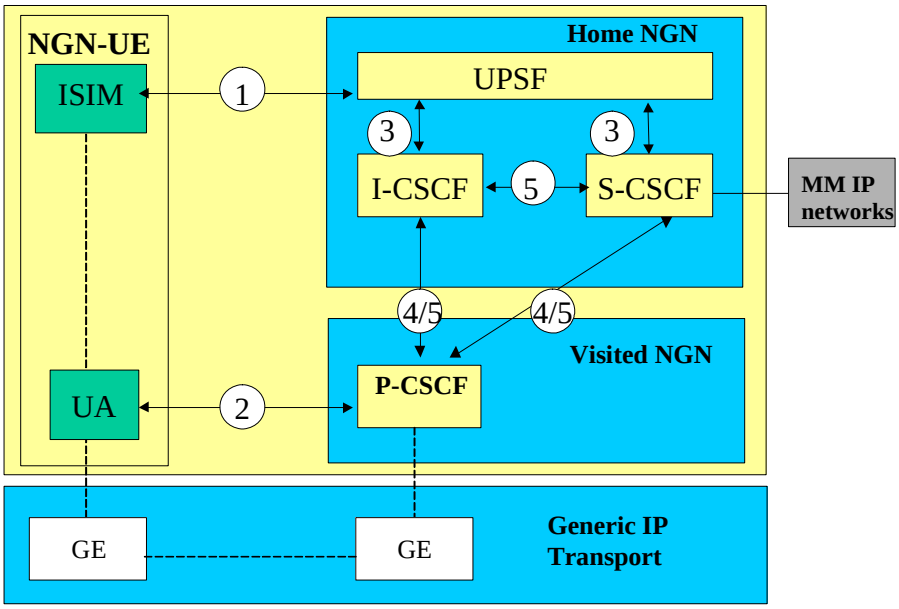


Figure 2: The IMS security architecture for fixed broadband access defined in TS 133 203 [i.15]

For the five different security associations defined for security protection in the IMS shown in Figure 2 there is no relationship between the Transport domain and the IMS domain but only the following associations for the relationship of the NGN user and the NGN core network are considered:

1) Provides mutual authentication between the HSS (through the S-CSCF as a proxy) and the UE. The long-term key in the ISIM and the HSS is associated with the IMPI and the key is exchanged only by means of the UICC containing ISIM.

2) Provides a secure link and a security association between the UE and a P-CSCF for protection of the Gm reference point and the IMS (SIP) signalling it carries where Ipsec ESP is the protection mechanism used.

NOTE 2: A pair of associations is created between the source IP address of the UE and the destination IP address of the P-CSCF, and between the source IP address of the P-CSCF and the destination IP address if the UE. The associations are identified by different (and ideally system unique) SPI values.

In addition to the explicit relationships considered above there are implicit relationships for protection of the user managed within the network and provided by the Ipsec functionality of Network Domain Security described in TS 33.210 [i.20]. The NDS functionality explicitly protects the following points shown on Figure 2:

1) Provides security within the network domain internally for the Cx-interface.

2) Provides security between different networks for SIP capable nodes and is only applicable when the P-CSCF resides in the Visited Network.

3) Provides security within the network internally between SIP capable nodes and applies when the P-CSCF resides in the HN.

Whilst other interfaces and reference points exist in IMS there is no explicit points user centred security association and any protection of data of user data is solely determined by the application of NDS by the operators.

The specific security features offered for IMS are as follows:

- Secure access to IMS:
  - Authentication of the subscriber and the network:
    - Applied to the IMPI as principal associated with a shared secret that is pre-configured on the UICC.

NOTE 3: Whilst the UICC is mandated in the body of TS 133 203 [i.15] to be in the UE it is also allowed for non-UMTS access to be provided in the IMS Residential Gateway (see Annex L of TS 133 203 [i.15]).

  - Re-Authentication of the subscriber.
  - Confidentiality protection:
    - Applied between the UE and P-CSCF (point 2 on Figure 2) using the confidentiality key derived during ISIM authentication and applied to Ipsec ESP for protection of all signalling at IP between the UE and the P-CSCF.
  - Integrity protection:
    - Applied between the UE and P-CSCF (point 2 on Figure 2) using the integrity key derived during ISIM authentication and applied to Ipsec ESP for protection of all signalling at IP between the UE and the P-CSCF.
- Network topology hiding:
  - The operational details of an operator's network are sensitive business information that operators are reluctant to share with their competitors. While there may be situations (partnerships or other business relations) where the sharing of such information is appropriate, the possibility should exist for an operator to determine whether or not the internals of its network need to be hidden.

For the confidentiality and integrity services defined in TS 133 203 [i.15] the Ipsec security associations require knowledge of the IP addresses of the UE and P-CSCF to be exchanged to allow the Sas to be established. A broad assumption in the IMS/UMTS infrastructure is that the algorithm set is common for key derivation (i.e. to generate the cipher key (CK) and the integrity key (IK)). In the IMS domain CK and IK are used with Ipsec ESP to establish a tunnel between the UA and the P-CSCF. This requires that private data (cryptographic keys) belonging to the IMS (ECS) domain is shared with the Transport (ECN) domain and each domain may be maintained by distinct providers.

NOTE 4: This vulnerability (sharing of private data) is common to all SIP environments that rely upon security from the transport domain.

NOTE 5: It is noted that it is possible that keys used to protect SIP signalling (CK and IK) on Ipsec may also be used in the UMTS connection.

8.4 Resolution protocols in NGN

8.4.1 DNS and ENUM

The role of DNS, and of ENUM as a specialisation of DNS, is to map a name to an address. From a security and privacy perspective as DNS was not originally designed with security in mind it has evolved with a number of security issues. A TVRA of ENUM (incorporating DNS) is given in TR 187 002 [i.11].

The ENUM and DNS entries contain data that may reveal private data. As the nature of ENUM and DNS is to share data.

8.5 NGN Authentication, Registration and Authorization

8.5.1 Overview

The NGN is a multi-provider network infrastructure where there may be a large number of access providers and service providers. This makes it particularly difficult to protect identities and identity-related information while ensuring that behavioural details cannot be linked to true identities. A multi-provider environment requires the exchange of identity and addressing information so that services can be delivered to the requesting user and that user is correctly charged for the services consumed.

Identity information and behavioural details must be both protected for privacy reasons and traced to enable service delivery and charging. Therefore, the NGN must be extended with three conceptual models for identity protection and accountability. The first model handles authentication, registration and forwarding of identity information in the NGN. The second model is the authorization model based on PMI protecting identity and identity related information during service requests and consumption. The third model is an extension to PMI for audit purposes to ensure that NGN users can be held accountable for their actions whilst being protected against identity crime. This means that identification, authentication, authorization and accountability in NGN require the two following mechanisms that each record data for audit:

1) registration; and

2) authorization.

8.5.2 NGN Authentication and Registration

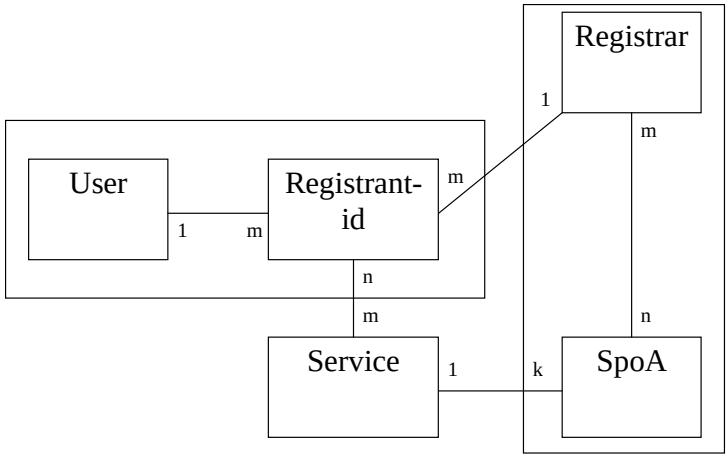
FFS.

8.5.3 NGN Authorization

NOTE: A model for access control is given in TS 102 165-2 [i.10] that is extended here for NGN authorization.

The primary purpose of the NGN Authorization (as a form of access control) service is to counter the threat of unauthorized invocation of operations on the communications system. The use of access control is often considered to explicitly counter threats and their associated threat agents that lead to attacks of unauthorized use, disclosure, modification, destruction and denial of service.

Authorization counter-measures act independently of authentication and confidentiality countermeasures but are used to determine if the identity (confirmed through authentication) is authorized to use the service requested. Figure 3 shows a view of the access control problem wherein a user, represented by the NGN user identifier, is offered access to many services at potentially multiple attachment points.



NOTE 1: A single user may be associated with many registrant-ids.
NOTE 2: A registrant-id shall be associated with only one user.
NOTE 3: A registrant-id shall be associated with only one registrar.
NOTE 4: A registrar may be associated with many registrant-ids.
NOTE 5: A service may be associated with many SpoAs.
NOTE 6: In any registration instance a service shall be associated with only one SpoA.
NOTE 7: An SpoA shall be associated with only one Service.
NOTE 8: A registrant-id may be associated with many Services.

Figure 3: Ordinal relations in the NGN

On receipt of a request to access a service from a known entity shall be validated against the access policy maintained for the service. The access policy may be applied in a number of ways:

- all requests conforming to a pattern have access;
- requests conforming to a pattern from authorized parties have access (white list);
- requests conforming to a pattern from known unauthorized parties are denied access (black list).

If the requestor is not allowed access to the named service access shall be denied.

In the event of any protocol failure no access shall be granted.

The generic model for an access control system consists of 3 functional elements:

- Access requestor:
  - The entity requesting access to a specific network entity.
- Access policy verifier:
  - The entity that checks to see if the requestor is allowed to access the specific network entity and which instructs the policy enforcer to enable/disable access.
- Access enforcer:
  - The entity that enables or disables access to a resource for the access requestor under control of the policy validator.

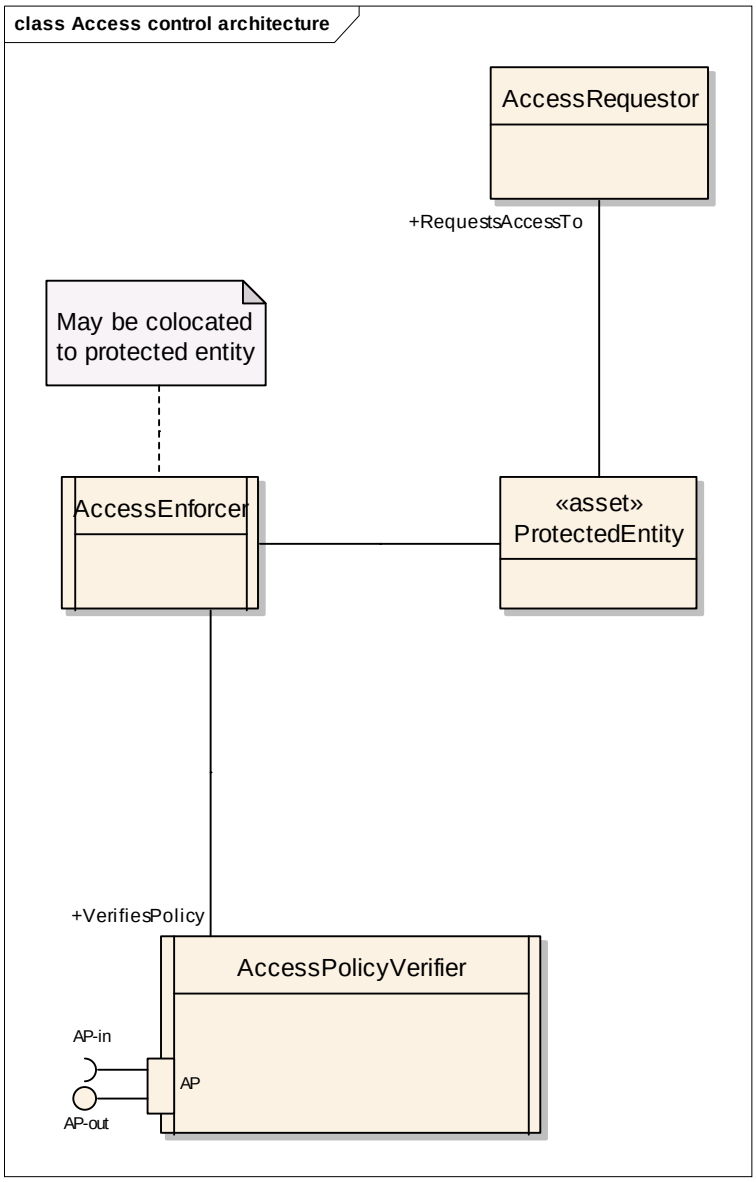


Figure 4: Pattern for access control mechanism

There are a number of deployment models that offer different protection and performance opportunities. The model offered in figure 5 places the access enforcer as a firewall-like entity that intercepts every input to the protected asset, validates it and either forwards it or rejects it.

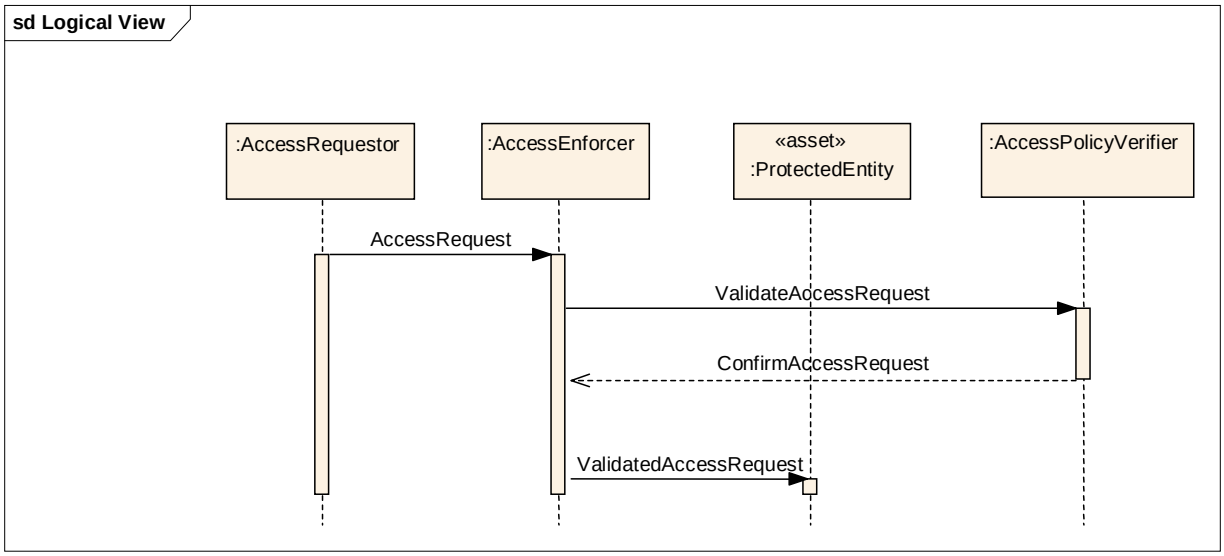


Figure 5: Interaction diagram for access control pattern (firewall mode)

The firewall model may be applied in a number of ways:

- all requests conforming to a pattern have access;
- requests conforming to a pattern from authorized parties have access (white list);
- requests conforming to a pattern from known unauthorized parties are denied access (black list).

8.6 Gap analysis

FFS.

8.7 Detailed requirements

FFS.

Annex A (normative): Protection Profile Proforma for Identity Protection in the NGN

Protection Profile					
Introduction					
Doc No.	TS 187 016	Version	3.1.1	Date	2010-06
Full Title	Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Identity Protection (Protection Profile)				
Overview	The present document specifies countermeasures to assure that users of the NGN have protection from abuse of identity. This covers authenticity and integrity countermeasures, including use of existing systems, and credential management in support of identity protection. The present document: • identifies the security objectives, • defines the functional requirements (including those from ISO/IEC 15408-2 [i.6] that apply), • defines the detail requirements for protection of identity in the NGN. In doing so the present document: • defines measures that provide protection of the NGN user identity from malicious traffic analysis; • identifies those measures that allow compliance with the privacy legislation in the regions where the NGN is to be deployed where such legislation is known and public. • identifies in annex B a number of countermeasures in the form of policies or procedures. The present document follows the recommendations of ES 202 382 [2] and provides an IdM PP Proforma which may be used as a basis for developing a PP for identity protection in an NGN subsystem deployment. The identity protection PP proforma is provided in Annex A.				
TOE Description					
See Annex D.					

Protection Profile		
TOE Security Environment		
a.1 Assumptions		
a.1.1	SIP is the primary signalling system used within the NGN	Annex D
a.1.2	The UE connects to the NGN at three distinct logical points (Transport, IMS/Service, Application)	Annex D
a.1.3	The transport attachment is a normal IP termination	Annex D
a.1.4	it is possible to invoke end-user services directly at the transport layer	Annex D
a.1.5	It is possible to bypass any service normally connected at either the IMS/Service or Application layers by direct IP access	Annex D
a.2 Assets (See clause 8.1 and annex D as a basis.)		
a.2.1		
a.2.2		
a.3 Threat agents (See clauses 4 and 5 and TR 187 010 [i.19] as a basis.)		
a.3.1		
a.3.2		
a.4 Threats (See clauses 4 and 5 and TR 187 010 [i.19] as a basis.)		
a.4.1		
a.4.2		
a.5 Security policies (OPTIONAL)		
a.5.1		
a.5.2		
Security Objectives		
1	Access to NGN services should only be granted to users with appropriate authorization	Clause 4
2	The identity of an NGN user should not be compromised by any action of the NGN	Clause 4
3	No action of the NGN should make an NGN user liable to be the target of identity crime	Clause 4
4	No change in the ownership, responsibility, content or collection of personal data pertaining to an NGN user should occur without that user's consent or knowledge	Clause 4
5	Personal data pertaining to an NGN user should be collected by the NGN using legitimate means only	Clause 4
6	An audit trail of all transactions having an impact on personal data pertaining to NGN users should be maintained within the NGN	Clause 4
7	The identity of an NGN user should not be compromised by any action of the NGN	Clause 4
8	No action of the NGN should make an NGN user liable to be the target of identity crime	Clause 4
9	The NGN shall comply with the European regulations on privacy (EC Directives 2002/58/EC [4] and 2006/24/EC [5])	Clause 4
10	The NGN shall comply with the European regulations on data protection (EC Directive 95/46/EC [7])	Clause 4
11	The NGN shall comply with the requirements to support law enforcement (EC Directive 2006/24/EC [5] and COM 96/C329/01 [6])	Clause 4

Protection Profile			
c IT Security Requirements (See table 1 in clause 6.1 as a basis.)			
c.1 TOE security requirements			
c.1.1 TOE security functional requirements			
c.1.1.1			
c.1.1.2			
c.1.2 TOE security assurance requirements (This is business and market segment specific. See ISO/IEC 15408-3 [i.13] for guidelines.)			
c.1.2.1			
c.1.2.2			
c.2 Environment security requirements (OPTIONAL)			
c.2.1			
c.2.2			
d Application notes (OPTIONAL)			
e Rationale			

Annex B (informative): Policy and Procedure countermeasures

It should not be possible to determine the identifier associated with a particular NGN user by observation or knowledge of another unrelated NGN user. For example, there should be no direct correlation between the NGN identifiers of two fixed line subscribers living in adjacent houses.

Annex C (informative): Security terms and concepts

C.1 Security associations

The detail design of security in the context of UPM (and user profiles in general) requires consideration of the security associations between objects, i.e. those relationships between objects that are open to attack and which are protected by the provisions of the architecture. Such associations exhibit a number of properties with respect to security and have to be considered in the overall design. Security associations are:

- Links that determine assurance.
- Links that determine security functionality.

A security association defines:

- Algorithms used for each security capability.
- What security capabilities are available.
- What keys are to be used.

C.2 Confidentiality

The aim of confidentiality measures are to ensure that communication between Alice and Bob, if intercepted by Eve, remains confidential. In other words Eve cannot access the content of the communication.

C.3 Integrity

The aim of integrity measures is to provide assurance that text has not been modified.

The method of operation of an integrity protection and validation mechanism generally involves the following steps:

- Prepare a digest of the text at source.
- Prepare a digest of the text at the destination.
- Compare it to a digest of the text calculated at the destination.

If the digests are the same there is a high assurance that there has been no manipulation of the text in transit. The aim of any cryptographic algorithm for integrity is to give assurance that the integrity check sum can only be generated from the original text and that any change in the text will result in a different integrity check sum (i.e. relies on inability of attacker to create a matching check value with random tools and data).

C.4 Authenticity

The aim of authenticity measures are to prove that Ann is really Ann with the intention to make it difficult for Bob to masquerade as Ann. The person or entity being authenticated is termed the Principal and authentication methods rely upon something that the Principal **is**, **has** or **knows:**

- Is = Biometric data.
- Has = Token, smartcard.

- Knows = Password.

This is sometimes supplemented by how the principal does things (behaviour). The methods of achieving authentication fall into two root classes (for cryptographic authentication):

- Challenge - response:
  - The authenticator challenges the authenticate, who responds, and the authenticator checks the response. The method relies on inability of an attacker to guess the correct response even with knowledge of the challenge and the algorithm used to generate the response.
- Keyed digest:
  - Process some data using tools only the transmitter should have to give a summary, send it. If the receiver can only match the summary using matching tools then it was created and sent by the transmitter. Relies on inability of attacker to create a match with random tools and data.

C.5 Authority

Authority is the ability to answer the question "is Anne allowed to that?" where "allowed" is a statement of Anne's authority. In many computer systems files have attributes of Read, Write, Delete (and others) and the rights of the user determine which of these capabilities are available to each user. In a more distributed environment such as in telecommunications the assertions of authority are more complex and require some form of Authority Management Infrastructure (AMI) which can be found in two main suites of protocols and objects:

- Security Assertion Markup Language (SAML).
- Privilege Management Infrastructure (PMI) in X.509 Attribute Certificates.

For both SAML and PMI authority, and its validation, may be described as follows:

- Authority A was issued at time t by issuer R regarding subject S provided conditions C are valid.

A pre-requisite of authority validation is authentication, and that itself has a pre-requisite of identification.

Annex D (informative): Privacy in the NGN - TVRA

D.1 Identification of the ToE

The concept of a Target of Evaluation (ToE) in security analysis [i.6] is used to set the boundary for an analysis and for specifying the goal, purpose and scope of the analysis. The identification of the ToE is part of producing the inventory of the assets (step 3) of the TVRA method.

The ToE specifies the scope of the analysis, describes the assets and their relations, and provides a focus for the analysis. For the purposes of the Identity Protection TVRA, the ToE has been identified as the NGN itself with only the NGN user in the uncontrolled ToE environment.

The ToE environment is used to specify the communicating entities associated with possible attack interfaces into the ToE. This is shown in Figure D.1.

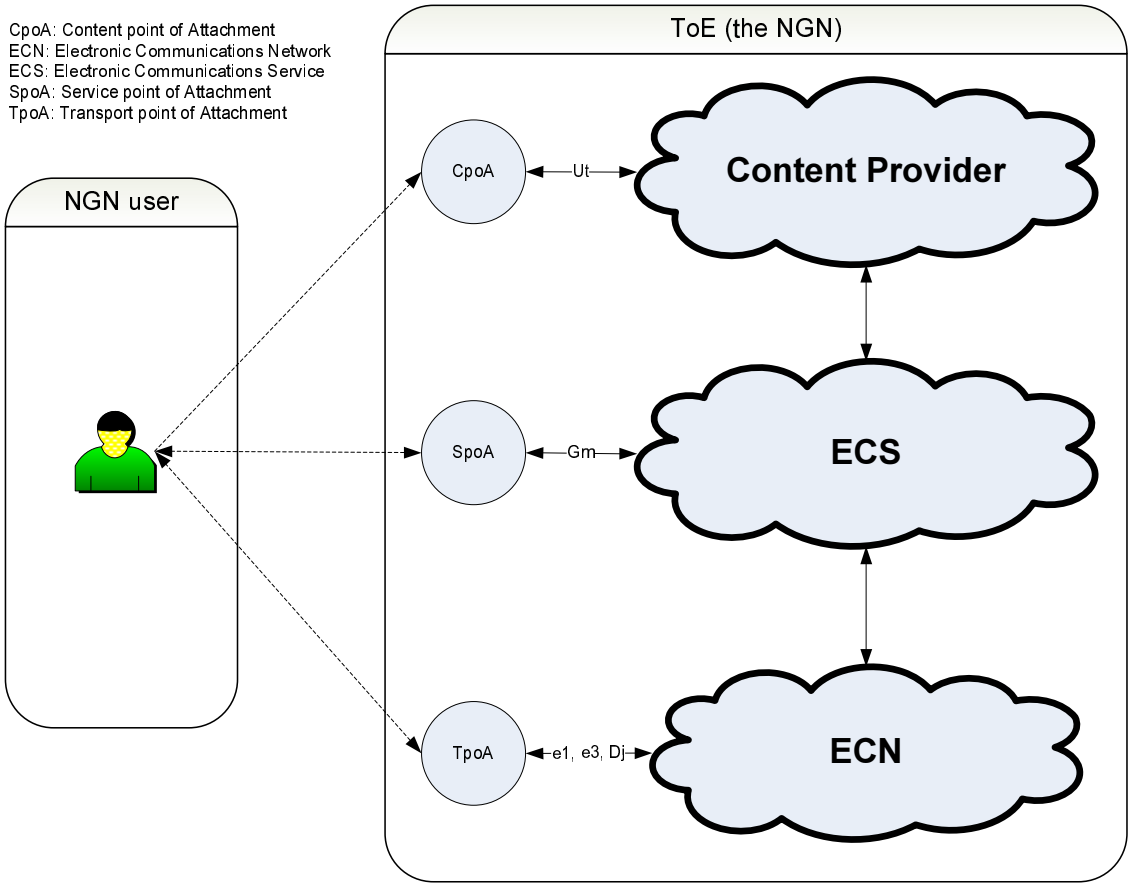


Figure D.1: Identification of ToE

For the purposes of analysis the NGN is considered based on the ECN&S structure identified in the framework directive and inside the NGN the main reference points that equate to the ECN, ECS and Content Provider elements are identified as below:

- To ECN: e1 and e3 for address allocation, authentication and authorization;
- To ECN: Dj for sending and receiving media and media control flows;
- To ECS: Gm for access to IMS;
- To Content Provider: Ut.

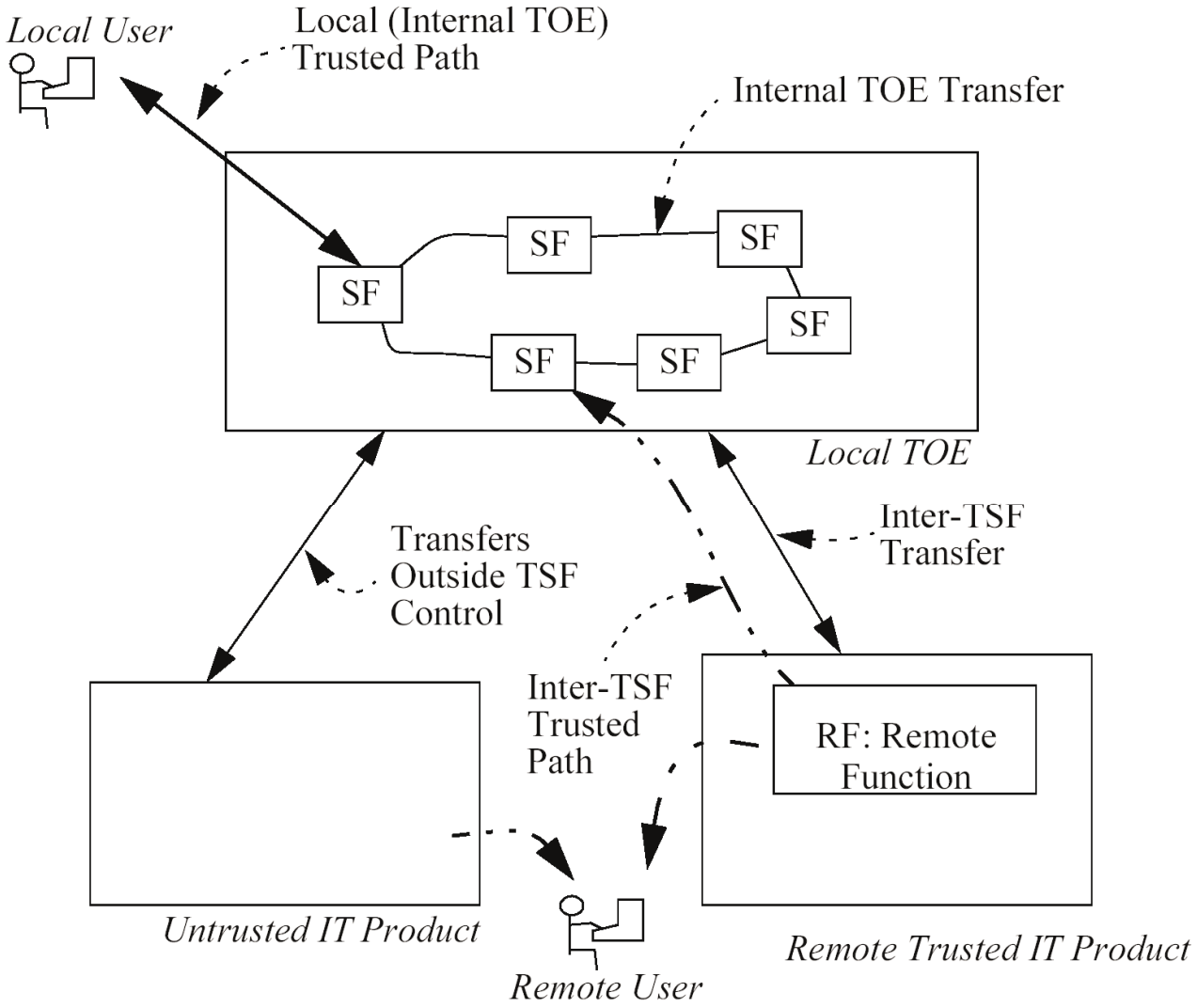


Figure D.2: Overview of distributed ToE from ISO/IEC 15408-2 [i.6]

D.2 Observations on the ToE

There is a very strong relationship between IMS AKA and UMTS as defined in clause 6 of TS 133 203 [i.15] and there is a unstated inference that UMTS-AKA and IMS-AKA share a common primary secret as they share the mechanisms for generation of the authentication vector.

SIP is one of a class of protocols called Representational State Transfer (REST) that refer to a variant of client-server architecture for distributed systems. The concept of REST is of a request-response dialogue between the client and server where the state of the interaction is not held on the server, but forms a client side only state machine whose current state is communicated to the server with each request. In the NGN use of SIP the responses from the server (the CSCFs) indicate to the client (the UE) the expected content of the next SIP message. This means that the conventional Authentication-challenge, Authentication-response, Authentication-result stage 2 information flows are implemented in SIP using the following messages (see TS 133 203 clause 6.1.1 [i.15]): SIP-Register (to bind IMPI and IMPU); 4xx Auth_Challenge (containing the challenge and keys within the trusted domain); SIP Register (containing the authentication response); 2xx Auth_OK (containing the result).

1) SIP is the primary signalling system used within the NGN and previous studies have demonstrated a number of core weaknesses in the SIP protocol [i.11];

2) The UE connects to the NGN at three distinct logical points (Transport, IMS/Service, Application) and the transport attachment is a normal IP termination it is possible to invoke end-user services directly at the transport layer and by that bypassing any equivalent service normally connected at either the IMS/Service or Application layers.

NOTE: The impact of any attack that exploits this weakness varies from the point of observation of the attack whereas the likelihood is constant.

Annex E (informative): Bibliography

ETSI TS 133 221: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Generic Authentication Architecture (GAA)".

ETSI TR 180 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Release 3 definition".

E.1 NGN

ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

E.2 RACS

ETSI ES 282 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture".

ETSI ES 283 018 (V2.7.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: H.248 Profile for controlling Border Gateway Functions (BGF) in the Resource and Admission Control Subsystem (RACS); Protocol specification".

ETSI TR 183 025 (V2.5.1): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); H.248 Non-call related procedures and management system interaction".

ETSI TS 183 048: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control System (RACS); Protocol Signalling flows specification; RACS Stage 3".

ETSI TS 183 017: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification".

ETSI ES 283 026: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification".

E.3 NASS

ETSI TS 183 019: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; User-Network Interface Protocol Definitions".

ETSI ES 283 034: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol".

ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

E.4 PSTN/ISDN Emulation

ETSI ES 282 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

E.5 IMS

ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description (3GPP TS 23.228 v7.2.0, modified)".

E.6 CPN

ETSI TS 185 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway Architecture and Reference Points".

ETSI TS 185 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN".

ETSI TS 185 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Devices architecture and Reference Points".

ETSI TS 185 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Premises Networks: Protocol Specification (Stage 3)".

E.7 TISPAN Adopted 3GPP specifications

ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102 Release 6)".

ETSI TS 133 141: "Universal Mobile Telecommunications System (UMTS); LTE; Presence service; Security (3GPP TS 33.141 version 8.1.0 Release 8)".

ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 Release 6)".

ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 Release 6)".

ETSI TS 129 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents (3GPP TS 29.228 Release 6)".

History

Document history		
V3.1.1	June 2010	Publication