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

Important notice

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

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

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

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

Copyright Notification

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.

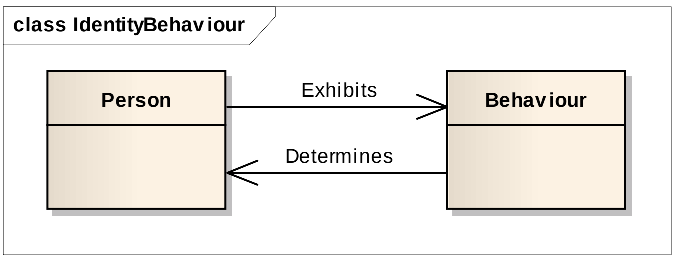

Figure 1: Link between person and behaviour

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.