ETSI TR 187 010 V2.1.1 (2008-07)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity management and their resolution in the NGN

Reference

DTR/TISPAN-07027-NGN-R2

Keywords

management, 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

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 Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document summarizes the work that is ongoing in relation to management of trusted identifiers (often referred to as the generic term Identity Management (IdM)) within a number of international standardization bodies and industry fora. From this summary, it identifies common themes which are relevant to IdM within ETSI's NGN activities and then presents the results of an IdM Threat Vulnerability and Risk Analysis (TVRA) based upon the method described in TS 102 165-1 [i.1].

The present document derives and presents a set of objectives and requirements for providing security of Identity and IdM in the NGN.

NOTE: The issues raised in the present document have been analysed with respect to the NGN but apply equally to existing and alternative telecommunications networks.

2 References

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

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

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

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

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

2.1 Normative references

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

Not applicable.

2.2 Informative references

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

[i.1] 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] 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".

[i.3] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[i.4] ETSI TS 184 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Identifiers (IDs) for NGN".

[i.5] ETSI TS 188 002-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network and Service Management; Subscription Management; Part 2: Information Model".

[i.6] ETSI TS 102 165-2 (V4.1.1): "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures".

[i.7] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)".

[i.8] ETSI TR 184 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Number Portability scenarios in Next Generation Networks (NGNs)".

[i.9] ETSI EG 284 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks (NGN)".

[i.10] ETSI EG 201 940: "Human Factors (HF); User Identification solutions in converging networks".

[i.11] ETSI EG 202 067: "Universal Communications Identifier (UCI); System framework".

[i.12] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[i.13] 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).

[i.14] UK Home Office; R.V.Clark; "Hot Products: understanding, anticipating and reducing demand for stolen goods", ISBN 1-84082-278-3.

[i.15] Recommendation of the OECD Council in 1980 concerning guidelines governing the protection of privacy and transborder flows of personal data (the OECD guidelines for personal data protection.

[i.16] ITU-T Recommendation E.164 (02/2005): "The international public telecommunication numbering plan".

[i.17] ISO/IEC 17799 2005: "Information technology - Security techniques - Code of practice for information security management".

[i.18] 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.19] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.20] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.21] AS/NZS 4360: "Risk Management".

[i.22] Directive 2002/21/EC of the European Parliament and of the council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[i.23] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal service and users' rights relating to electronic communications networks and services (Universal Service Directive - OJ L 108, 24.04.2002).

[i.24] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

[i.25] 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. .

[i.26] ETSI TS 133 220: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220 version 7.11.0 Release 7)".

[i.27] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[i.28] IETF RFC 2821: "Simple Mail Transfer Protocol (SMTP)".

[i.29] NIST, FIBS-PUB 180-2: "Secure Hash Standard".

3 Definitions, and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EG 202 387 [i.2], ISO/IEC 17799 [i.i.17], ISO/IEC 13335-1 [i.18] 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.18]

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

Concealable, Removable, Available, Valuable, Enjoyable, and Disposable (CRAVED): acronym for a classification scheme to determine the likelihood that a particular type of item will be the subject of theft [i.14]

Identifier: series of digits, characters and symbols used to identify uniquely subscriber, user, network element, function or network entity providing services/applications

Identity: identifier allocated to a particular entity, e.g. a particular end-user, provides an Identity for that entity (TS 184 002 [i.i.4])

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

identity fraud (1): use of a false identity or legitimate identity to support unlawful activity

identity fraud (2): falsely claiming to be a victim of identity theft to avoid obligation or liability

identity theft: event that occurs when sufficient information about an identity is obtained to facilitate identity fraud

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

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

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

spam: bulk unsolicited communication where the benefit favours the sender

residual risk: risk remaining after risk treatment

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

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

NOTE 1: A threat consists of an asset, a threat agent and an adverse action of that threat agent on that asset (reference [i.19]).

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: an entity that can adversely act on an asset

unwanted incident: incident such as loss of confidentiality, integrity and/or availability (reference [i.21])

user: person or process using the system in order to gain access to some system resident or system accessible service

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

NOTE: A **Vulnerability**, consistent with the definition given in ISO/IEC 13335 [i.18], 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:

AKA	Authentication and Key Agreement
BSF	Bootstrap Server Function
CLIP	Calling Line Identity Presentation
COLP	Called Line Identification Presentation
CPE	Customer Premises Equipment
CRAVED	Concealable, Removable, Available, Valuable, Enjoyable, and Disposable
CSP	Communications Service Provider
ECN	Electronic Communications Network
ECN&S	Electronic Communications Networks & Services
ECS	Electronic Communications Service
GAA	Generic Authentication Architecture
GBA	Genetic Bootstrap Architecture
HSS	Home Subscriber Server
IdM	Identity Management
IdP	Identity Provider
IMEI	International Mobile Equipment Identity
IMS	Internet protocol Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
LAP	Liberty Alliance Project
NAF	Network Application Function
NAI	Network Access Identifier
NASS	Network Access SubSystem
NP	Number Portability
NT	Network Termination
OASIS	Organization for the Advancement of Structured Information Standards
PDU	Protocol Data Units
PES	PSTN Emulation Subsystem
PIP	Personal Identity Portability

R&TTE	Radio equipment & Telecommunications Terminal Equipment
RACS	Resource and Admission Control Subsystem
RP	Relying Party
SDO	Standards Development Organization
SIM	Subscriber Identity Module
SLF	Subscriber Locator Function
SPIT	SPam over Internet Telephony
SpoA	Service point of Attachment
SuM	Subscription Management
TpoA	Transport point of Attachment
TVRA	Threat Vulnerability and Risk Analysis
UCI	Universal Communications Identifier
UE	User Equipment
UPM	User Profile Management

4 Review of IdM

4.1 Overview

The identity of a human individual is generally considered to be non-transferable and to have the same lifetime as the individual. The unauthorized use of a person's identity by a third party can have considerable short term as well as long term financial and societal consequences for the victim. The European privacy directive 2002/58/EC [i.13] addresses the legal obligations of users and providers to preserve a user's control of their identity when used in electronic communication (specifically to counter bulk unsolicited communication), whilst the R&TTE directive [i.24] requires protection of personal data (which may be a component of identity) when such data is embedded in terminal devices.

The role of identity in communications networks is one that is not well understood. Identity in the wider, societal use of the term, is not the same as the concept of identity used in telecommunications which is the collection of identifiers, permissions and authentication data necessary to gain access to services. Most current telecommunications identification schemes use a single identifier to perform (at least) two distinct functions, namely:

- routing:
  - identifiers can be processed by information and communication systems to enable end-to-end service instances between end-points to be established;
- identification:
  - end-users can identify the source of an incoming communication (e.g. CLIP, email addresses) or confirm the identity of the remote end-point to which a connection has or will be established (e.g. COLP, urls).

Failure of the first of these two functions may result in loss of service to end-users. To ensure that such failures do not occur, rules relating to the content and formatting of communication identifiers are enforced. As a result, most communications related identifiers have a defined structure which simplifies the identification of region, domain and/or end-point.

In many cases of attack on identity, countermeasures already exist, using corroborating data to reinforce the observation of an assertion of identity. Many organizations do not rely on a single identifier as an assertion of identity. Consequently, when trying to masquerade as a legitimate user, a criminal will seek to recover multiple correlated forms of identification and use them in combination to counter the identity checks. In those contexts where identity is represented by an identifier having a known structure (as is the case in email names [i.28] and the E.164 numbering [i.16] schemes) it is possible for the identity to be falsely claimed.

Identity management is an important aspect in overcoming current concerns regarding the definition of exactly what constitutes a user and what rights that user has. Unfortunately, as identity is a rather abstract concept, its management is difficult to define and specify.

4.2 Characterization of theft potential of identity

In order to determine whether identity is of value to a potential thief, it is useful to apply the CRAVED criteria [i.14] which have been developed to assess the risk of theft for specific disposable items as shown in table 1.

Table 1: CRAVED classification applied to identity

Criteria	Criteria clarification	Applicability to identity
Concealable	The target can easily be concealed by the thief or, at least, is not easily identifiable as not belonging to the thief	Yes. Identity is abstract so is concealed as a matter of course.
Removable	The target is not physically fixed or otherwise secured	Yes. If available an identifier can generally be copied, in some instances such as a removable SIM can be removed physically.
Available	The target is both visible and accessible to the thief	Yes. An identity becomes visible when used and its component identifiers and characteristics can be accessible in a number of ways (though not, necessarily, at a single location).
Valuable	The target has either intrinsic monetary value or personal value to the thief	Yes. Although an identity may not have any direct value in itself, it can be used to acquire other items and services which do have value to the holder.
Enjoyable	Possession of the target provides pleasure to the holder either through monetary or personal gain	Yes. Possession of an identity does not provide pleasure in itself but it can provide access to services and goods which the holder might find enjoyable.
Disposable	The target can be sold by the thief for monetary or other gain	Yes. Once all of its component identifiers and characteristics have been acquired, there is a ready market for them, particularly for the purpose of carrying out concealed criminal activities.

4.3 Regulatory protection of Identity

In addition to the CRAVED analysis it is useful to recognize the regulatory and legal frameworks in place to limit Identity Theft (and the resultant Identity Fraud). The European data protection directive 95/46/EC [i.25] and the privacy directive 2002/58/EC [i.13] state the legal obligations of both users and providers to preserve a user's control of their identity when used in electronic communication (specifically to counter bulk unsolicited communication). Similarly where radio equipment is deployed and where the R&TTE directive [i.24] applies, privacy of the identity has to be assured. This is explicitly cited in article 3.3 of the directive, as follows:

- apparatus of particular types shall be so constructed that:
  - it incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; and/or
  - it supports certain features ensuring avoidance of fraud.

In the United States of America "The Identity Theft and Assumption Deterrence Act (2003)" amended U.S. Code, s.1028 - "Fraud related to activity in connection with identification documents, authentication features, and information". The Code makes possession of any "means of identification" to "knowingly transfer, possess, or use without lawful authority" a federal crime, alongside unlawful possession of identification documents. Under the Act a name, birth certificate or US Social Security Number is considered a "means of identification". Similarly are credit card numbers, driver's licenses, an electronic serial number from a mobile phone (i.e. IMEI or IMSI) or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

4.4 Purpose of Identity and Identity Management in the NGN

An identity is used within the NGN to distinguish one NGN entity from another. The NGN entity may be an end-point (e.g. a telephone) or it may be service delivery agent (e.g. a service provider).

The purpose of Identity Management in the NGN is to control the life of an NGN identifier from its creation through assignment and, if necessary, reassignment, to its destruction at the end of its useful life. Identity Management may also include the maintenance of the integrity of an identifier.

NOTE: It is assumed that an NGN identifier is a machine processable token used to name an entity.

TS 184 002 [i.4] defines 3 classes of identifier which are not mutually exclusive:

1) Those generated automatically by network elements (e.g. call identifiers).

2) Those that may be allocated by operators without reference to external bodies (e.g. customer account number).

3) Those that are allocated to operators by external bodies (e.g. E.164 numbers, public IP addresses).

As only the identifiers in classes 2 and 3 are directly related to the end-user, it is these that may have value if stolen (see also the CRAVED analysis in table 1).

4.5 Identity portability

TR 184 003 [i.8] defines the requirements for supporting Number Portability (NP) or Personal Identity Portability (PIP) in the NGN and describes means of meeting these requirements. Where a CSP deploying an NGN is subject to the Universal Service Directive (2002/22/EC) [i.23], only NP is required and its implementation may be restricted. This may mean, for example, that is not possible to transfer a geographic number outside its defined geographical area.

4.6 Identity versus identifier

Telecommunications standards do not define identity but they do define identifiers which fall into any of the three (3) classes defined in TS 184 002 [i.4] (those generated automatically by network elements; those that may be allocated by operators without reference to external bodies; and those that are allocated to operators by external bodies).

An identifier is only one component of an NGN user's identity. As an example of how identifiers can be used in the construction of an identity, GSM associates a number of identifiers to each user and these combine with other items of information to form the user's complete identity within the context of GSM, thus:

- Identifiers:
  - IMSI, International Mobile Subscriber Identity:
    - identifies the SIM;
    - identifies the home system of the user (by Network and Country code elements of the IMSI);
    - used for registration and authentication only;
    - private identifier: Not published to other GSM users;
    - authoritative: ascribed during SIM manufacture;
  - IMEI, International Mobile Equipment Identity:
    - identifies the radio equipment;
    - used only in tracking equipment;
    - private identifier: Not published to other GSM users;
    - authoritative: ascribed during manufacture;