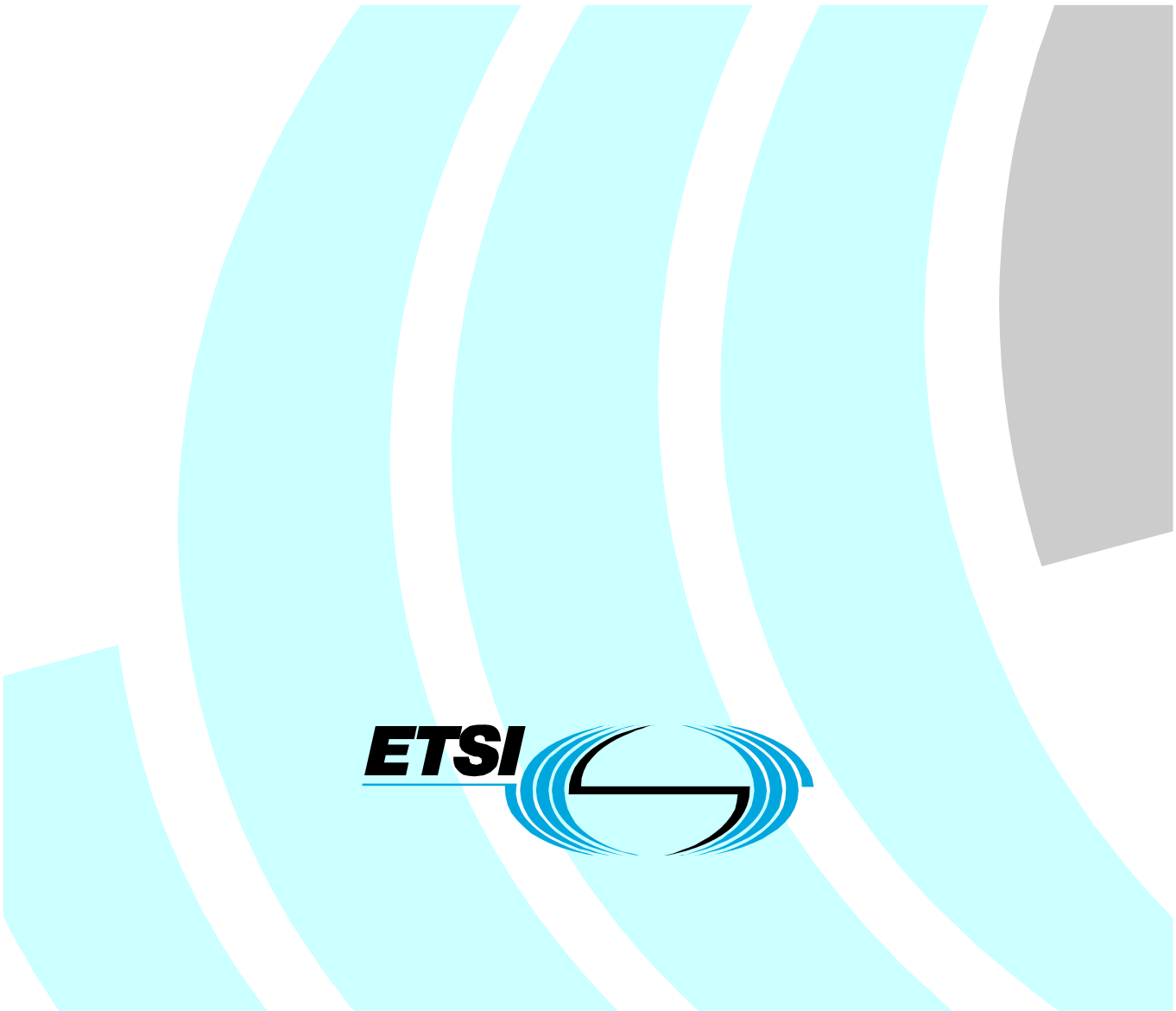
# ETSI TR 187 010 V2.1.1 (2008-07)

*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

# 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.<br>Identity is abstract so is concealed as a matter of course. |
| Removable | The target is not physically fixed or otherwise secured | Yes.<br>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.<br>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.<br>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.<br>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.<br>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;

- MSISDN, Mobile Subscriber ISDN number:
  - identifies the GSM subscriber;
  - used for directing calls (voice, fax, data, text) to and from the subscriber;
  - public identifier: published to other users (GSM or otherwise);
  - authoritative: ascribed by the subscriber's service provider;

- Other identity-related information:
  - passwords and access codes:
    - used to control access to the user's GSM handset;
    - non-authoritative: ascribed by the user;
  - authentication keys:
    - used at registration to validate the identity of the user's GSM equipment;
    - authoritative: ascribed by the manufacturer and unseen by the user;
  - user's service contract:
    - identifies services and tariffs available to the subscriber;
    - associated with the MSISDN rather than the GSM handset;
    - ascribed by the GSM service provider but can be changed frequently at the request of the subscriber.

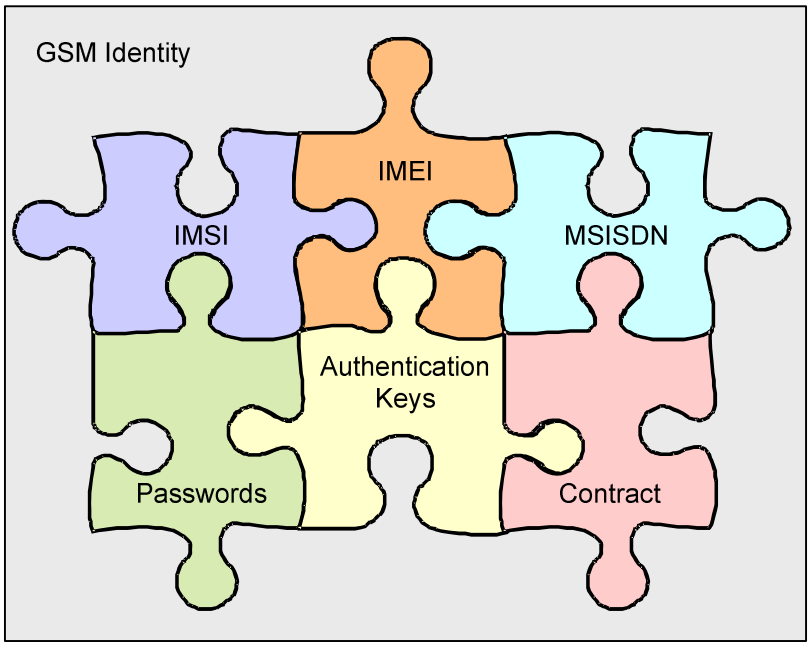



**Figure 1: Identity as a jigsaw puzzle of identifiers**

NOTE: The GSM identity is valid only in the context of GSM and does not claim to identify a particular person, only to identify that the handset is capable of legitimate use on the GSM network.

## 4.7 Principles for handling personal data in ICT networks

The OECD Guidelines for personal data protection [i.15] are closely related to the EC Data Privacy directives [i.13], and [i.25] and introduce a number of basic principles that, if adopted, may point towards a set of NGN IdM principles, thus:

- Collection limitation principle:
  - Limits to data collection:
    - Before collecting personal data - for example, when contracting with the data subject - an NGN operator should obtain the prior and unambiguous consent of the data subject or inform the data subject of the collection of personal data and the indicated purposes of use according to domestic regulations.
    - From the viewpoint of the NGN operator, consent is always required when personal data is used in commercial services. However, in cases of safety and public services, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provider.
  - Data collection methods:
    - An NGN operator should not acquire personal data by fraudulent or other dishonest means.
  - Data collection without consent:
    - The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation.
  - Exclusion of data capable of identifying an individual from collected data:
    - An NGN operator should take reasonable measures to avoid collecting data from which an individual could be identified by referring to a database in cases where such a possibility exists.
  - Confirmation of a data subject's consent about data collection:
    - An NGN operator should take suitable measures to confirm the consent of a data subject about data collection.
- Data quality principle:
  - An NGN operator should endeavour to keep personal data accurate and up to date within the scope necessary for the achievement of the purposes of use.
- Purpose specification principle:
  - Specification of the purposes of use:
    - When handling personal data, an NGN operator should specify the purposes of use of personal data.
- Limits on changing the purposes of use:
    - 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.
  - Change of the purposes of use required prior consent:
    - 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.

- Use limitation principle:
  - Use limitation:
    - 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.
  - Restriction of disclosure to third parties:
    - An NGN operator should not provide personal data to a third party without obtaining the prior consent of the data subject.
  - Use without consent:
    - The provisions of the preceding two paragraphs shall not apply to cases in which the handling of personal data is based on domestic laws. NGN operators should grant access only to law enforcement authorities as authorized by a domestic court order or equivalent legal instrument.
- Security safeguards principle:
  - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- Openness principle:
  - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of 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.
- Individual participation principle:
  - An individual may have the right to:
    - (a) obtain from an NGN operator, or otherwise, confirmation of whether or not the NGN operator has data relating to him;
    - (b) have communicated to him, data relating to him
      - (i) within a reasonable time;
      - (ii) at a charge, if any, that is not excessive;
      - (iii) in a reasonable manner; and
      - (iv) in a form that is readily intelligible to him;
    - (c) be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
    - (d) challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
- Accountability principle:
  - An NGN operator should be accountable for complying with measures which give effect to the principles stated above.

In addition to these principles derived from the OECD guidelines, the following can be derived from provisions in the Framework Directive [i.22] and in existing telecommunications practice:

- Equality of regime principle:
  - An NGN operator should not transfer personal data across borders unless the destination has an equivalent privacy regime as the origin.

- Anonymity principle:
  - An NGN operator should provide the means for users to transact anonymously.

The security safeguards principle and the individual participation principles lead to a strong requirement on ICT networks to manage identity and to be in a position to counter identity fraud.

# 5 IdM themes in other standardization bodies

## 5.1 Overview

Evidence of the growing importance of IdM can be found in the fact that governments, SDOs, manufacturers and academic institutes are all trying to develop legislative and technological counters to the problems of managing Identity mainly with a view to minimizing the incidence of Identity Fraud. An analysis of a number of these groups has been carried out in order to identify significant themes. The groups that were analysed and a summary of the findings are given in annex A.

## 5.2 Common thematic model

Three key IdM roles can be identified from an analysis of the ongoing work and output of a number of bodies active in the field:

- Principal:
  - Often synonymous with the end-user or an electronic agent of the end-user.
- Identity Provider (IdP):
  - The organization generally required to authenticate the Principal and to provide an assertion of this authentication to the Relying Party.
- Relying Party (RP):
  - An organization providing a service to the Principal. The Principal may authenticate to the RP but, the RP is also willing to rely on an assertion provided by the IdP.

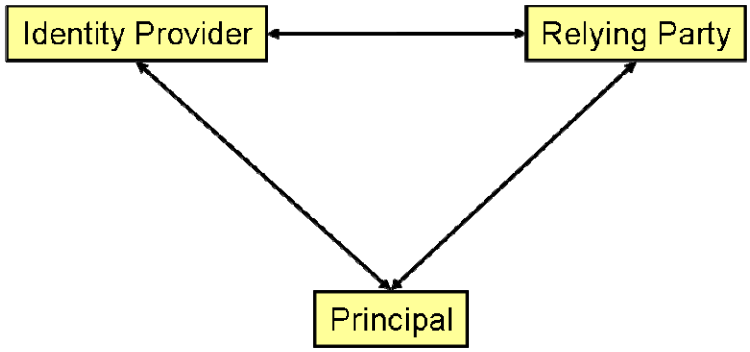



**Figure 2: The three primary roles in the common IdM thematic model**

While all IdM approaches analysed define these roles (sometimes the terminology used is different) they differ in the communication protocols used between these roles.

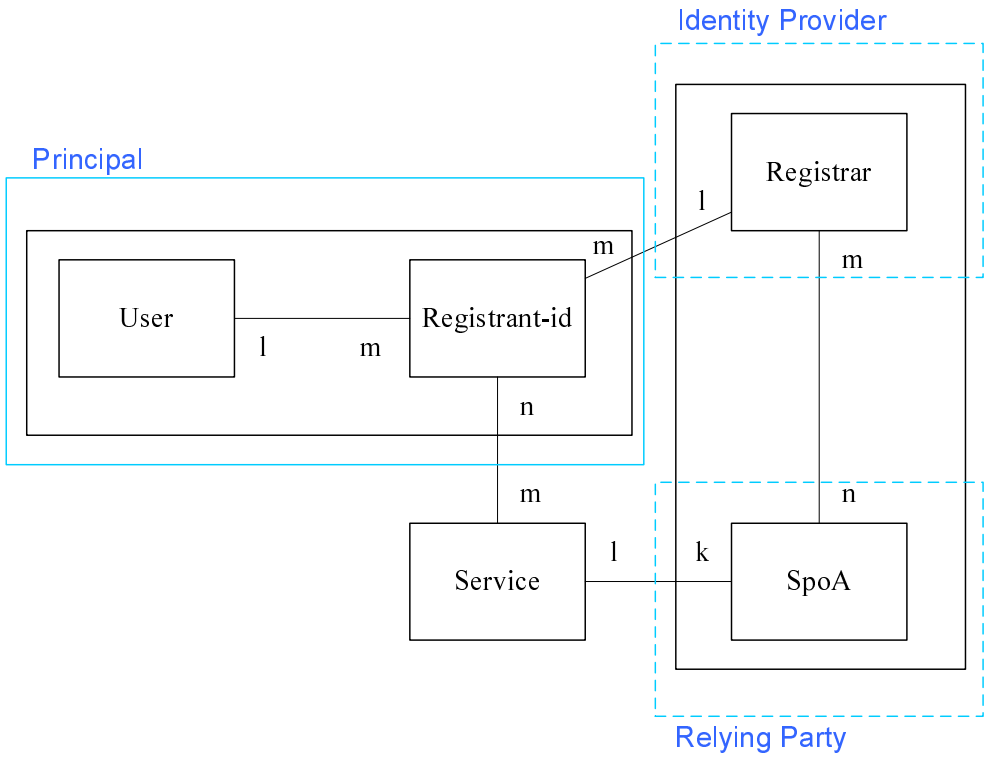
## 5.3 Common functional themes

### 5.3.1 Authorization

In all the systems and models examined identity is used as the key to unlock services or capabilities in the system. The key functional capability proposed is that users should be restricted prior to identification. The architectures for authorization are varied but include the following:

- single sign-on;
- federation;
- trust networks.

The authorization models used in the analyzed IdM activities are variations of the common thematic model shown in figure 2. In addition, the model derived by ETSI's TIPHON project [i.6] is fundamentally the same. The Principal in the TIPHON authorization model (shown in figure 3) is represented by the "User" combined with the "Registrant-id". The Identity Provider is represented by the "Registrar" and the Relying Part is represented by the "SPoA" (Service Point of Attachment).




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: The TIPHON authorization model**

### 5.3.2 Authentication

Authentication is a recurrent functional theme which is used as a reinforcement of identity prior to authorization. Authentication procedures are variously symmetric and asymmetric keyed schemes with both challenge-response protocols and digest based calculation or signature methods.

The authentication framework described in TS 102 165-2 [i.6] can be applied as a common model across the studied IdM initiatives. Whilst the text of TS 102 165-2 [i.6] is not repeated here, it is worthwhile highlighting one of its key points which is a recurrent theme in all of the analyses:

> Authentication methods rely upon something that the Principal **is**, **has** or **knows**, where each of these is considered as a class of information. Authentication that uses attributes from only one of these classes is referred to as "single factor authentication" while authentication that uses attributes from two or more of the classes is referred to as "multi-factor authentication".
>
> Typically, a human principal is identified by some form of biometric data and the assumption for authentication is that the biometric data is unique and cannot be forged.
>
> Authentication that is based upon something that the Principal possesses often makes use of a specific hardware module containing unique and non-forgeable secret information. This is the model used in mobile telephony (e.g. GSM) where the authentication key is held by the SIM which is inserted in a user's handset.
>
> The third class requires the user to provide known information to the authentication system. Such authentication includes the use of passwords, PINs and pass-phrases.
>
> In addition to the three classes described above, a fourth class is also possible to use an analysis of the behaviour of the authenticating entity as the basis for authentication.

### 5.3.3 Contextual uniqueness

An identifier has a specific meaning within a specific context and identity problems occur most frequently when either contexts are not unique or the scope of an identifier is extended beyond its original context (for example, by using a telephone number for something other than for making telephone calls). As elements of identity, identifiers are often used to support a claim of identity but such out-of-context uses of identifiers can generally be easily guessed in an identity fraud attempt. Where an identity can be restricted to a single purpose (with or without supporting authentication data) it may be more difficult to use it as the basis of identity fraud.

NOTE: In many cases it may not be practical to limit an identity to a single purpose as it would require retrospective modification of common practice. However, the principle should still be considered.

# 6 Identity in the NGN

## 6.1 Overview of the NGN

The NGN is a complex multi-platform system using a number of identifiers in a number of different ways. However, for simplicity the NGN can be considered to have 3 platforms, as follows:

- a transport platform containing the following subsystems:
  - network access management (NASS); and
  - resource and admission control (RACS).

NOTE: RACS does not perform an access control function as normally understood for security but instead ensures that the resources of the transport platform are managed with respect to the access request. Resource allocations are not directly dependent on the user identity but may be measured against subscription limitations identified in the subscriber profile (see the SuM model in clause 6.2.1).

- a service platform containing the following subsystems:
  - IP multimedia management (IMS); and
  - PSTN/ISDN emulation (PES).
- an applications platform.

## 6.2 IdM models relevant to the NGN

### 6.2.1 The Subscriber Management model

The Subscriber Management (SuM) information model defined in TS 188 002-2 [i.5] and shown in figure 4, identifies a hierarchy of identifiers which starts with the primary concept of a subscriber and incorporates a range of identifiers and identities that are associated with a user.

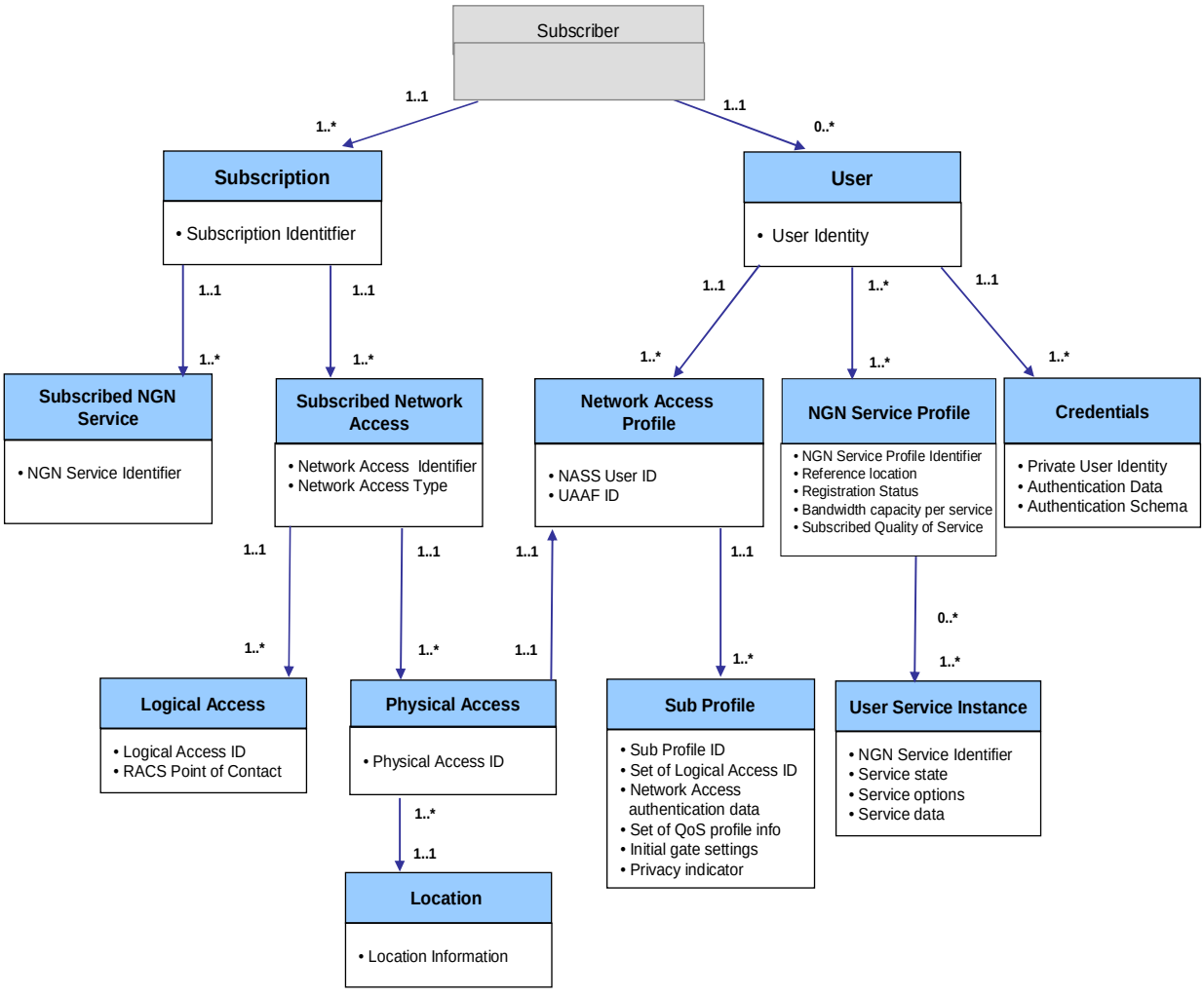



**Figure 4: TISPAN SuM High Level Model (from TS 188 002-2 [i.5])**

### 6.2.2 The ECN&S Model

The Electronic Communications Networks & Services (ECN&S) model defined in the EU Framework Directive [i.22] may also be analysed with respect to the use and management of identity. The ECN&S model (figure 5) shows both naming and addressing authorities with names (entity identifiers) belonging to the Electronic Communications Services (ECS) space, and addresses (entity locations) belonging to the Electronic Communications Networks (ECN) space.

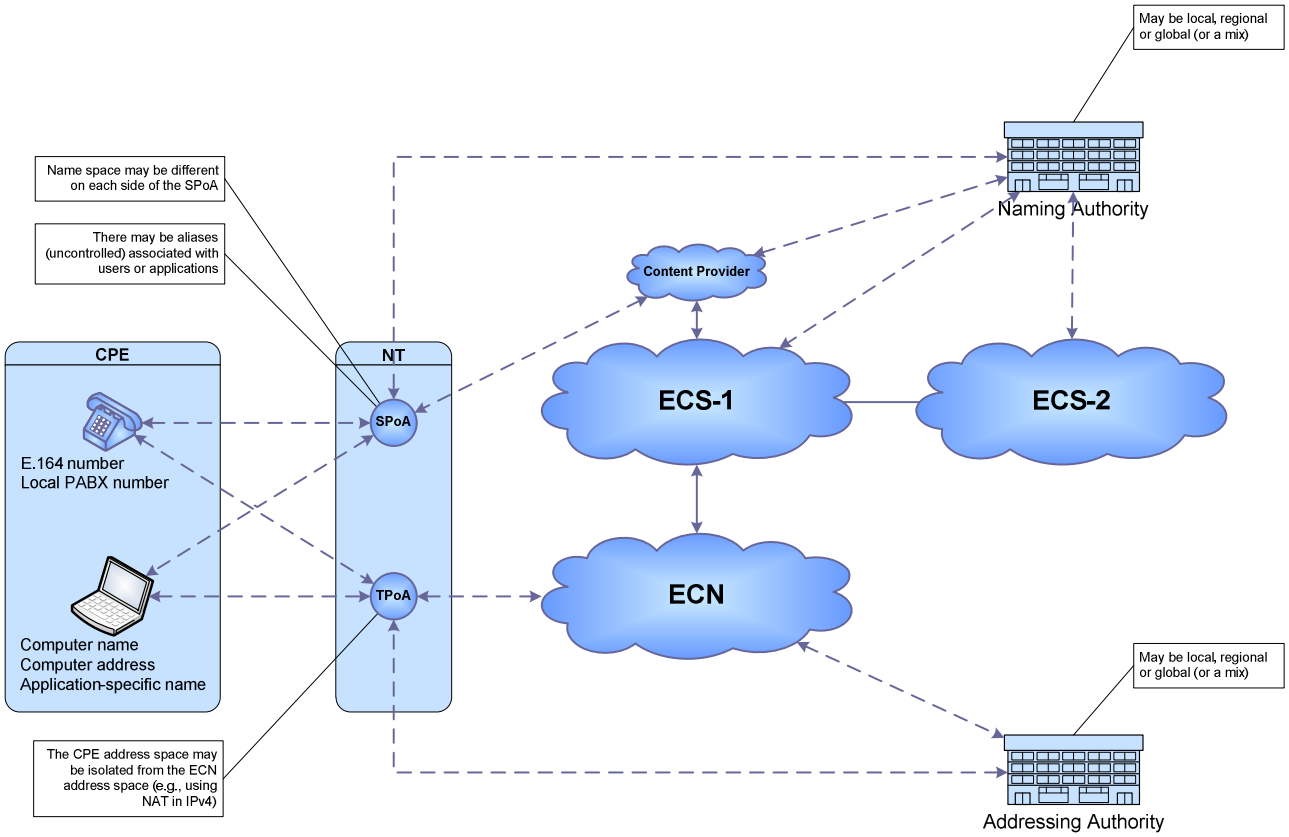



**Figure 5: Identity and IdM issues arising out of the ECN&S model**

### 6.2.3 The UCI model

The Universal Communications Identifier (UCI) model of Identity Management as described in EG 284 004 [i.9], EG 201 940 [i.10] and EG 202 067 [i.11] is similar to the SuM model but has been developed towards supporting user control of Identity.

The UCI model consists of a Personal User Agent that acts on behalf of the user and is able to interact with the services subscribed to by the user. The UCI capability fits into the service platform of the NGN and maintains separation of the user (in the ECS space) and the location of the user (in the ECN space).

## 6.3 The NGN transport platform

As the NGN transport platform is fundamentally an IP system, it recognizes the concept of addresses but does not incorporate the identification of specific users even though the combination of address and port may identify a particular NGN endpoint. The following identification information is used and maintained within the NGN transport platform:

- IP Address:
  - A logical identifier which is associated with the attached user equipment and which is unique within its addressing domain.
- Physical Access ID:
  - The identifier of the physical access to which the user equipment is connected.
- Static Information derived from the Physical access ID:
  - Location Information.
  - Default Subscriber ID.

- Logical Access ID:
  - The identifier of the logical access used by the attached user equipment. In the xDSL case, the Logical Access ID may explicitly contain the identifier of the port, VP and/or VC carrying the traffic.
- Static Information Derived from the Logical Access ID:
  - RACS point of contact: The address of the RACS element where the subscriber profile should be pushed.
  - Access Network Type: The type of access network over which IP connectivity is provided to the user equipment.

ES 282 004 [i.12] states "Network attachment through NASS is based on implicit or explicit user identity and authentication credentials stored in the NASS."

An identity must be used for access authentication. The identity used for explicit authentication may depend on the authentication mechanism applied and on the access network which the UE is connected to. Two examples of these identities are:

- user identity including credentials provided by the user;
- user equipment identity.

## 6.4 Service platform

Subscriber ID: The identity of the attached user.

## 6.5 Identity crime in the NGN

### 6.5.1 Identity theft

In the context of the NGN, the term, "identity theft" refers only to the unauthorized use of the set of NGN identifiers and other information which, together, characterize the identity of a specific NGN user. In contrast to the normal concept of theft where the target item is physically removed from the victim, identity theft generally involves capturing or copying identity details such that the legitimate owner may not even be aware of the theft.

The scale of identity theft is not accurately measured in all EU states. However government figures indicate a loss of approximately £372 million in the United Kingdom as a result of identity-related crime within the telecommunications industry during 2006.

### 6.5.2 Identity fraud

The NGN can be considered as a network that connects nodes where aspects of identity are made available. It is certainly possible that any links between the information held in such nodes would be unknown to the CSP operating the NGN even if the means to establish communication between the nodes are known. As an example, if a single user has access to both a bank server and a social networking server there may be sufficient information held in the social networking server to provide a criminal with the means to commit identity fraud within the bank server. The NGN or the CSP operating the NGN may not be in a position to prevent such fraud.

### 6.5.3 The NGN as a barrier to identity crime

The NGN can only act as a barrier to identity crime in those instances where it is responsible for access to or generation of data that could be used in committing the crime.

## 6.6 NGN security objectives related to IdM

The primary objective of any secured system is to avoid the occurrence of unwanted incidents.

As stated in clause 4.4 the purpose of Identity Management in the NGN is to control an identifier throughout its lifetime from its creation to its ultimate destruction. An analysis of the OECD guidelines (clause 4.7), the common IdM development themes in other standardization bodies (clause 5) and the potential for identity crime in an NGN (clause 6.5) identifies the set of objectives listed in table 2.

**Table 2: Security objectives related to IdM in the NGN**

| OBJ | 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 IdM Threat, Vulnerability and Risk Analysis (TVRA)

## 7.1 TVRA overview and introduction

In order to be able to identify suitable countermeasures within the NGN to avoid or, at least, limit the impact of breaches in identity security, it is necessary to analyse the potential threats, vulnerabilities and risks that exist in this area. TS 102 165-1 [i.1] specifies the method used here for carrying out a Threat, Vulnerability and Risk Analysis (TVRA).

The primary objective of this analysis is to identify potential unwanted incidents in the context of Identity and IdM in the NGN and to propose countermeasures which would reduce or obviate the likelihood of such incidents occurring.

## 7.2 Unwanted incidents relating to Identity and IdM in the NGN

### 7.2.1 Unauthorized creation of identities

The unauthorized creation of identifiers may lead to unauthorized use of NGN services leading to the following unwanted incidents:

- in the transport platform:
  - unauthorized creation of Transport related identifiers, either IP identifiers or identifiers in the NASS, may lead to unauthorized network access;
  - unauthorized creation of an excessive number of identifiers may lead to a denial of service and a reduced availability for authorized users (e.g. a DHCP IP allocation depletion attack).
- in the service platform:
  - unauthorized creation of service identifiers may lead to unauthorized use of NGN services.

### 7.2.2 Unauthorized destruction of identities

The unauthorized destruction or removal of NGN-related identities will lead to an unauthorized denial of service for the user whose identifiers have been removed or destroyed.

- in the transport platform:
  - unauthorized deletion of a user's transport related identifiers will lead to a denial of service (a loss of availability) for this user;
  - unauthorized deletion of part of a user's transport related identifiers may lead to a loss of accountability or repudiation, i.e. the NGN ECN operator might not be able to charge the user.
- in the Service platform:
  - unauthorized deletion of a user's service related identifiers will lead to a denial of service (a loss of availability) of NGN services for this user;
  - unauthorized deletion of part of a user's service related identifiers may lead to a loss of accountability or repudiation, i.e. the NGN ECS operator might not be able to charge the user for the services provided by the NGN.

### 7.2.3 Transfer of responsibility for identities and identifiers between CSPs

If a CSP transfers responsibility for a user's identity or identifier without the express authorization of the user, this could result in:

- loss of availability or denial of service for the end-user;
- unauthorized disclosure of sensitive information.

### 7.2.4 Masquerade

The use of an identity by anyone other than its true "owner", generally referred to as masquerade, is one of the main threats in any identity-based communication system. A masquerade attack can only be successful if the relying party is unable to distinguish between the true claimant and a false one.

#### 7.2.4.1 Self-revealing and non-self-revealing masquerade

Although it is rarely possible to identify a masquerade attack at the time that it takes place, the results of the attack may or may not reveal that it did, in fact, occur. Masquerade attacks that are revealed by their results are generally referred to as "self-revealing" while those that do not are referred to as "non-self-revealing". Examples of both types of masquerade attack are given below:

- Self revealing masquerade:

  Financial crime:

  Bob subscribes to an NGN service from a CSP by impersonating Peter. Bob uses Peter's personal identifiers that he has somehow acquired. The resultant crime reveals itself when Peter receives a demand for payment for the service from the CSP.

- Non-self revealing:

  Concealment crime:

  Bob impersonates Peter by using his personal identifiers in order to access confidential information to which he is not legitimately entitled. Neither Peter nor his NGN CSP is likely to be aware of Bob's crime.

### 7.2.5 Traffic analysis to obtain behavioural patterns

Identifiers may be observed remotely to gather significant data about the holder of the identifier and its usage. Such data may include details of the servers and services accessed and any regular patterns of behaviour. Although this information may not be sufficient for a criminal to mount an identity-related attack, it may make it easier for the criminal to avoid detection. Where an identifier is used in a single context (one service/one identity, as opposed to one identity/many services) the gain from analysis is minimized. However the NGN is adopting a model of one identity/many services and there is a risk that behavioural patterns may be analysed by observation of identifiers over time. Schemes to mitigate this using temporary identities are commonly used in radio systems.

Traffic analysis can also lead to the ability of an attacker to correlate identities together and to infer knowledge of one identity from another. Where identity is tied to services such as presence and location information patterns of behaviour may reveal the true identity even if a temporary identity is offered.

## 7.3 IdM assets

The hierarchy of IdM assets is complex as each asset may be contained in a system element which is also an asset. At the lowest level of analysis an asset may be considered as atomic with increasingly complex layers of containment above. A single atomic level asset may be present in multiple containers. As an example, an information element may exist in several Protocol Data Units (PDUs), several PDUs may be used in a single protocol and several protocols may exist in a single device (see figure 6). For the purposes of IdM TVRA, the atomic level is considered to be an identifier.

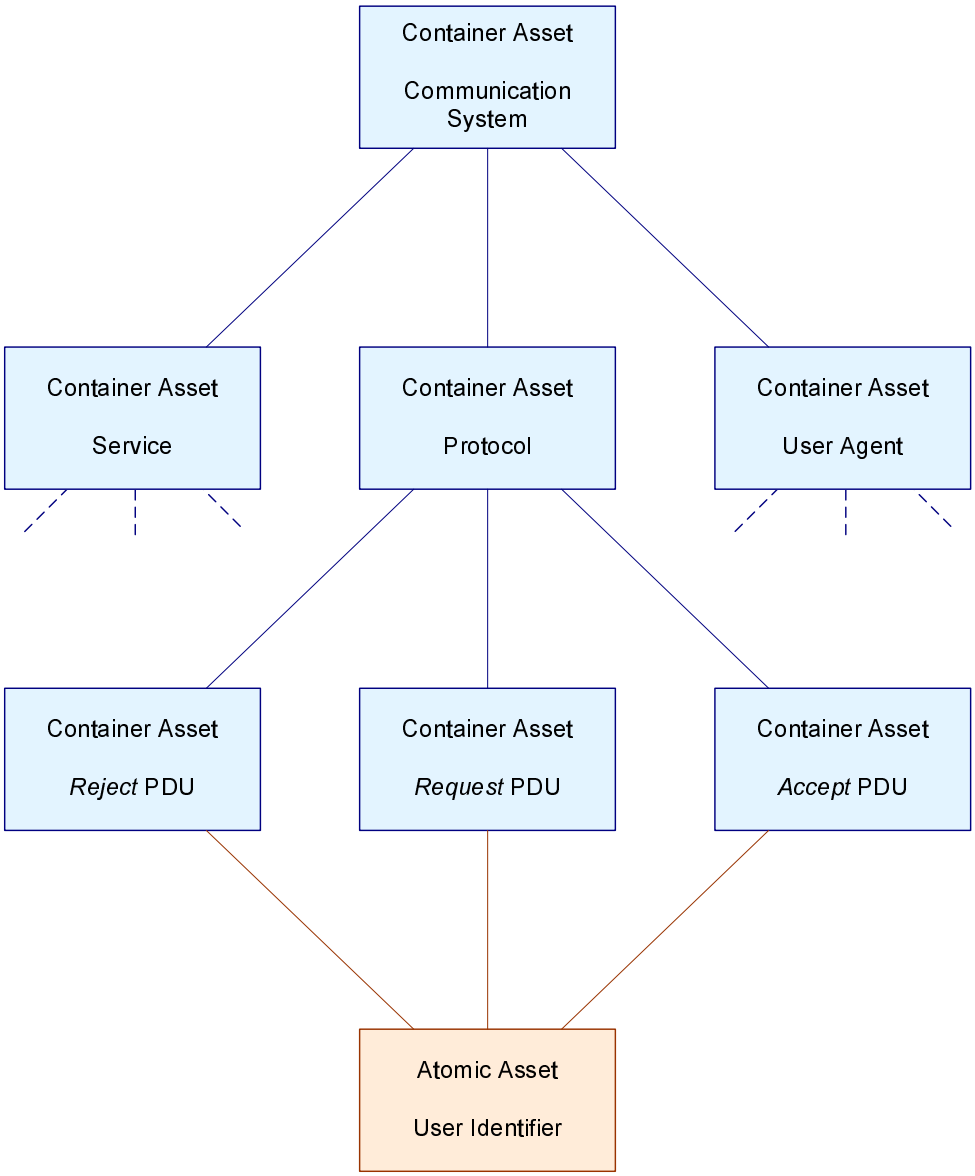



**Figure 6: Asset hierarchies in an abstract model**

### 7.3.1 Mapping of IdM assets to NGN

Atomic IdM assets (or contained assets) are deployed in physical assets (or container assets) and the combinations considered in the analysis are shown in table 3.

**Table 3: Examples of pairings of atomic assets and their container assets**

| Atomic asset | Container asset |
|---|---|
| SIP URI | SIP Protocol<br>INVITE<br>REGISTER |
| Tel URI | SIP Protocol<br>INVITE<br>REGISTER |
| IP address | SIP Protocol |
| IMPU | SIP Protocol |
| IMPI | SIP Protocol |
| E.164 telephone number | ENUM |
| SIP URI | ENUM |
| Personal URI | ENUM |
| SIP URI | IMS AKA |
| TMSI, IMSI | UMTS AKA |

## 7.4 Vulnerabilities in NGNs with relevance to IdM

A vulnerability is exposed when both a weakness and a threat able to exploit that weakness exists. A class 2 or class 3 identifier which is transported and, thus, made visible end to end (i.e. to the communicating parties) constitutes a weakness that is open to exploit by any end point. Furthermore, as the identity is offered to the network without validation and as SIP is able to add an alias (in a similar way to many instant messaging programmes), the use of communications networks by end-users may violate some of the recommendations made for NGN operators.

If an end user is able to use a self-asserted identifier (e.g. an alias) then there are no capabilities offered in the NGN standards to protect or manage it.

The core weaknesses of the NGN are as follows:

- data is transferred en-clair;
- data stores can be accessed through multiple channels.

The main threats are those that allow observation of identifiers in transit or in storage. It is important to recognize that if an identifier is used as described in clause 4.1, it must be visible. The use of NGN-identifiers by end-users can only be managed using non-NGN mechanisms.

## 7.5 IdM Risk assessment

### 7.5.1 Masquerade

#### 7.5.1.1 By mimic of structure of NGN identifiers

The structure of all identifiers in the NGN is public knowledge as is the assignment of many of the codes within the structure. Consequently, it is a trivial exercise for an attacker to create an identifier which has a valid structure. It is, however, considerably more difficult for a user to insert such an identifier into the NGN protocols or for an attacker to derive any benefit from such an attack.

The impact of an attack by mimicry is considered low and to have no significant impact either to NGN users or to NGN networks. Furthermore any attempt to counter an attack by concealing the structure of NGN identifiers, particularly those in classes 2 and 3, could render the NGN unusable.

#### 7.5.1.2 By capture of NGN identifier on NGN interfaces (eavesdropping)

The overall NGN architecture (from ES 282 001 [i.3]) shows 3 interfaces from the user to the NGN:

- Applications, at reference point Ut.
- Services, at reference point Gm (for IMS services via the P-CSCF).
- Transport, at reference points e1 (NASS via ARF to AMF), and e3 (to CNGCF).

In practice, as the NGN is designed to offer services over a common IP transport infrastructure, all of the reference points are visible at a single physical interface and, thus, carry the same risk of attack by eavesdropping .

The ability of an attacker to capture an NGN identifier on an NGN interface is dependent on the protection given to signals on NGN interfaces and, in particular, the protection of information elements within signals. Nevertheless, in principle, it is a reasonably simple task to intercept the signalling in an NGN call and to extract user identifiers from it.

An attack by capture, by itself, is unlikely to have any significant impact either on NGN users or on NGN networks. However, the impact of a successful interception and capture of signalling data may be more significant if it is subsequently used as the basis for a traffic analysis. In such a case, an attacker may be able to deduce the communications behaviour related to a specific identifier (where the identifier is indicative of a real person) and thus use that additional behavioural information to launch a successful masquerade attack at a later time.

## 7.6 IdM risk classification

The risk associated with a particular type of attack is determined by considering the likelihood of such an attack (assuming that a potential attacker is fully motivated to mount an attack) and its impact on the users and operators of the NGN. Table 4 summarizes the risks assessed for each of the attack types analyzed in clause 7.5.

**Table 4: Summary of NGN attack risks**

| Attack type | | Likelihood | Impact | Risk |
|---|---|---|---|---|
| Masquerade | Mimic of structure of NGN identifiers | High | Very low | Low |
| Eavesdropping | Capture of NGN identifiers at Ut reference point | High | Very low | Low |
| | Capture of NGN identifiers at Gm reference point | High | Very low | Low |
| | Capture of NGN identifiers at e3 reference point | High | Very low | Low |

## 7.7 IdM countermeasure framework

### 7.7.1 Counter to masquerade

Masquerade attacks are conventionally countered by the use of authentication. Within the NGN there are a number of authentication schemes specified. The applicability of each scheme depends on the form of access network and on the form of the service platform.

The success of authentication as a countermeasure is strongly linked to the means by which keys are managed as opposed to the particular algorithm or protocol implemented.

#### 7.7.1.1 Policy measures

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.

#### 7.7.1.2 Service platform

In those cases where IMS acts as a service platform, the authentication scheme defined in TS 133 203 [i.7] applies. The authentication identifier is the IMS Private User ID (IMPI) in the form of a Network Access Identifier (NAI).

### 7.7.2 Counter to eavesdropping

Eavesdropping may be countered by encryption (confidentiality protection). Within the NGN there are a number of encryption schemes specified. The applicability of each scheme depends on the form of access network and on the form of the service platform.

## 7.8 Functional security requirements

The list of NGN functional security requirements shown in table 5 is derived from an analysis of both the security objectives (table 2) and the risks associated with IdM in the NGN (table 4). For each requirement, a functional class (as defined in ISO/IEC 15408-2 [i.20]) is identified and this is used in the development of functional security requirements for the NGN.

**Table 5: IdM functional security requirements**

| | Functional requirement | Functional class (from ISO/IEC 15408-2 [i.20]) |
|---|---|---|
| **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 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 generated 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 | |
| 2.2 | The identity of the identity provider should not be retrievable from analysis of a class 2 identifier | Unobservability |
| 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 | |
| 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 |
| 2.5 | 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 |
| **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 |

| | Functional requirement | Functional class (from ISO/IEC 15408-2 [i.20]) |
|---|---|---|
| 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 |
| **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 |

NOTE 1: The functional components specified in ISO 15408-2 [i.20] provide a good basis for the specification of detailed requirements for secure equipment but do not adequately cover the requirements for protecting network users' personal data in transit. Consequently, the components identified in table 5 should not be considered as comprehensive.

NOTE 2: The list of functional requirements shown in table 5 is the result of only a cursory analysis of the derived objectives and serves primarily as an example rather than a comprehensive specification.

### 7.8.1 Modified IdM risk classification

When the countermeasures and functional classes are implemented in the NGN the overall risk for IdM is modified as the likelihood of any attack type is minimized. This is shown in table 6 which modifies the content of table 4.

**Table 6: Modified NGN attack risks after countermeasure application**

| Attack type | | Likelihood | Impact | Risk |
|---|---|---|---|---|
| Masquerade | Mimic of structure of NGN identifiers | High | Low | Low |
| Eavesdropping | Capture of NGN identifiers at Ut reference point | Low | Low | Low |
| | Capture of NGN identifiers at Gm reference point | Low | Low | Low |
| | Capture of NGN identifiers at e3 reference point | Low | Low | Low |

# Annex A:
# An analysis of IdM activities in non-ETSI bodies

## A.1 ITU-T

### A.1.1 Overview

The objectives of the ITU-T SG17 Focus Group on Identity Management (FG IdM) are to prepare a set of deliverables that include:

- a living list of standards bodies, forums, and consortia dealing with Identity Management, including information concerning their activities and documents in the context of an IdM framework;
- a global analysis on IdM requirements and capabilities; and
- a set of IdM telecommunications/ICT use cases that can be used to derive requirements.

In carrying out these objectives, the Focus Group may analyze other aspects related to the objectives (e.g. frameworks). FG IdM understands the term IdM as "management by providers of trusted attributes of an entity such as subscriber, a device, or a provider". This is not intended to indicate positive validation of a person.

In summary, the objectives of the FG IdM are:

- to perform requirements analysis based on uses case scenarios;
- to identify generic IdM framework components;
- to complete a standards gap analysis;
- to identify new standards work that ITU-T SGs and other SDOs should undertake.

### A.1.2 ITU-T FG IdM

ITU-T's FG IdM has undertaken a broad review of IdM standardization developments within SDOs and industry fora with a view to avoiding duplication and identifying (and, ultimately, filling) any gaps in the overall IdM standardization programme. As a result, this group is following no obvious themes that do not exist elsewhere. However, at the current early stage of their work, the following areas of particular interest have been identified:

- the specification of a common IdM architecture:
  - functional blocks;
  - interfaces;
  - protocols;
  - interoperability.
- specification of a common identity discovery method across:
  - groups;
  - networks;
  - technologies;
  - communities.

One of the results of the FG IdM work is an Identity Ontology and this is shown graphically in figure A.1.

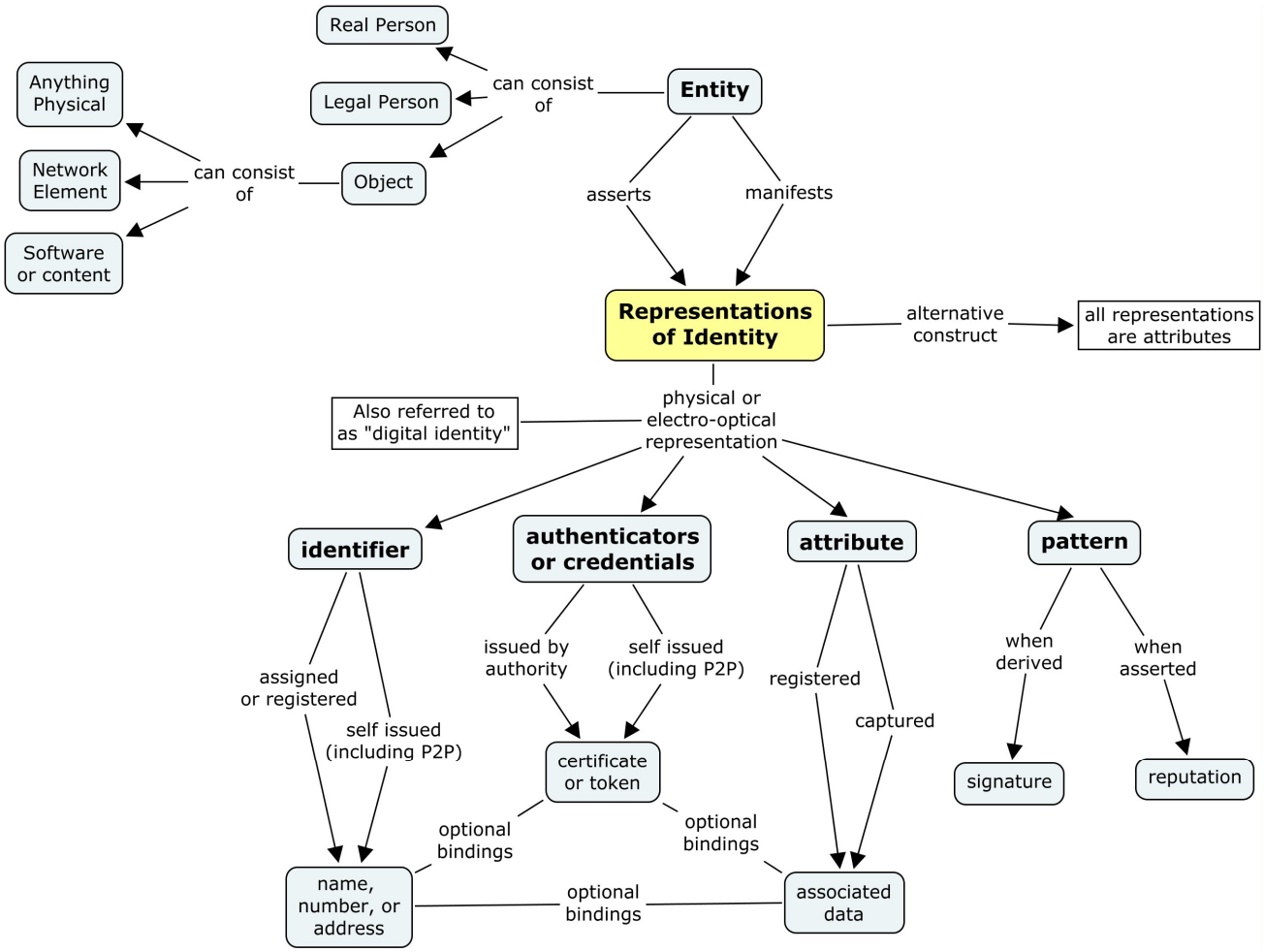



**Figure A.1: ITU-T FG IdM Identity Ontology**

A further output of the ITU-T FG IdM an examination of how Identity Management fits into the wider world of protection in the context of cyber-security as illustrated in figure A.2.

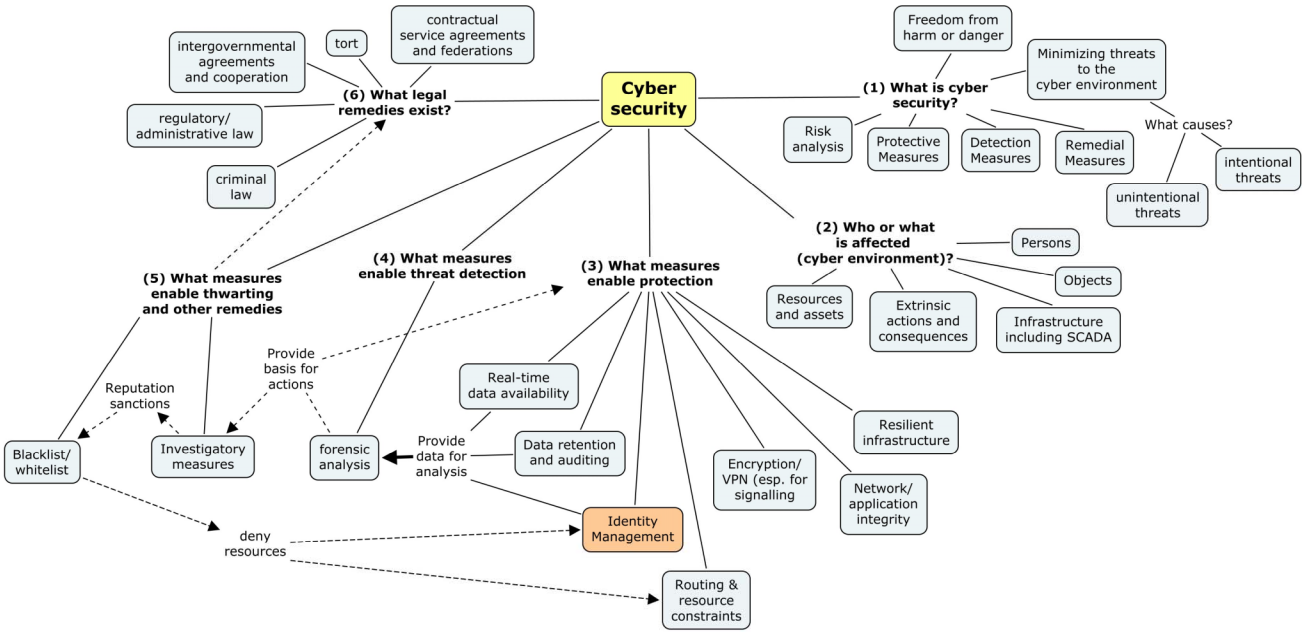



**Figure A.2: ITU-T FG IdM placement of IdM with respect to Cyber Security**

# A.2 3GPP

## A.2.1 Overview of activities

The 3rd Generation Partnership Project is responsible for the standardization of post-GSM cellular radio technology. One of the fundamental 3GPP building blocks is the IP Multimedia core network Subsystem (IMS) which is also central to the NGN architecture.

In a 3GPP system, IdM is used in combination with authentication and single sign-on procedures to control access by mobile terminal users to services in its core network.

## A.2.2 Current IdM work themes

As identity management is an important aspect of its access control philosophy, there are a number of activities related to IdM within the 3GPP work programme. These include:

- the specification of a Generic Authentication Architecture (GAA) and its associated procedures;
- the use and support of Subscriber Certificates;
- the migration of 2nd Generation mobile identifiers into GAA;
- the interworking of the GAA with the Liberty Foundation Identity Web Service Framework (ID-WSF).

## A.2.3 The Generic Bootstrapping Architecture (GBA)

The 3GPP Generic Bootstrap Architecture (GBA) identifies the entities involved in registering (and authenticating) User Equipment (UE) on start-up. This architecture is shown in figure A.3 . The components involved are the HSS, BSF (Bootstrapping Server Function), NAF (Network Application Function), SLF (Subscriber Locator Function), and UE. (The SLF is not required in a single HSS environment or when the BSF is configured to use a pre-defined HSS). In the architecture in figure A.3 it is assumed that the NAF and the BSF are in the same network domain (the home network of the subscriber). The architecture can be extended to allow the possibility for the NAF to reside in a visited network [i.26].

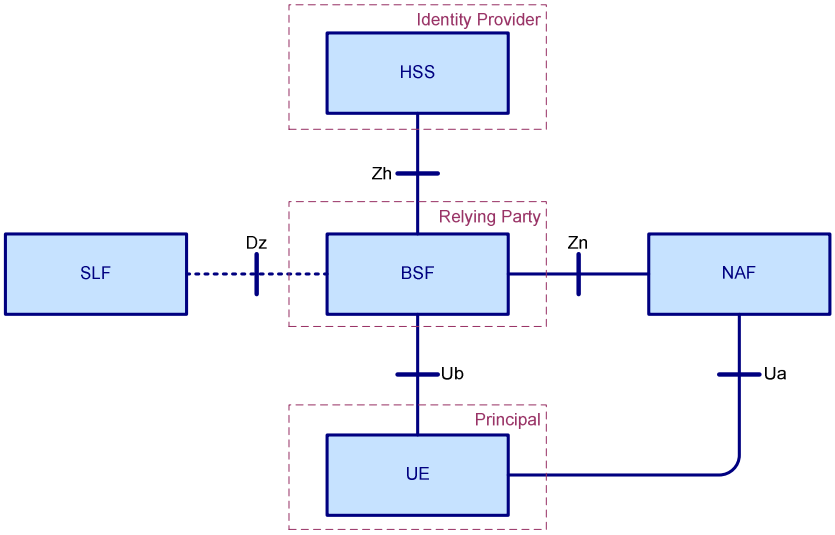



**Figure A.3: GBA Architecture**

The Bootstrapping Server Function and the UE mutually authenticate using the AKA protocol at the Ub reference point, and agree on session keys that are afterwards applied between the UE and a Network Application Function (NAF). This bootstrapping procedure is shown in figure A.4. After the bootstrapping procedure, both the BSF and the UE are able to construct a shared master key *Ks*, as the concatenation of the *CK* and *IK* keys that are obtained as a result of the AKA procedure.

After bootstrapping both the UE and the BSF use *Ks* to derive the key material *Ks_(ext/int)_NAF*. This is used to secure the communication between the UE and a particular NAF. The key derivation procedure is based on HMAC-SHA1-256 as specified in NIST FIBS Publication 108-2 [i.29] and RFC 2104 [i.27]. Further details can be found in TS 133 220 [i.26].

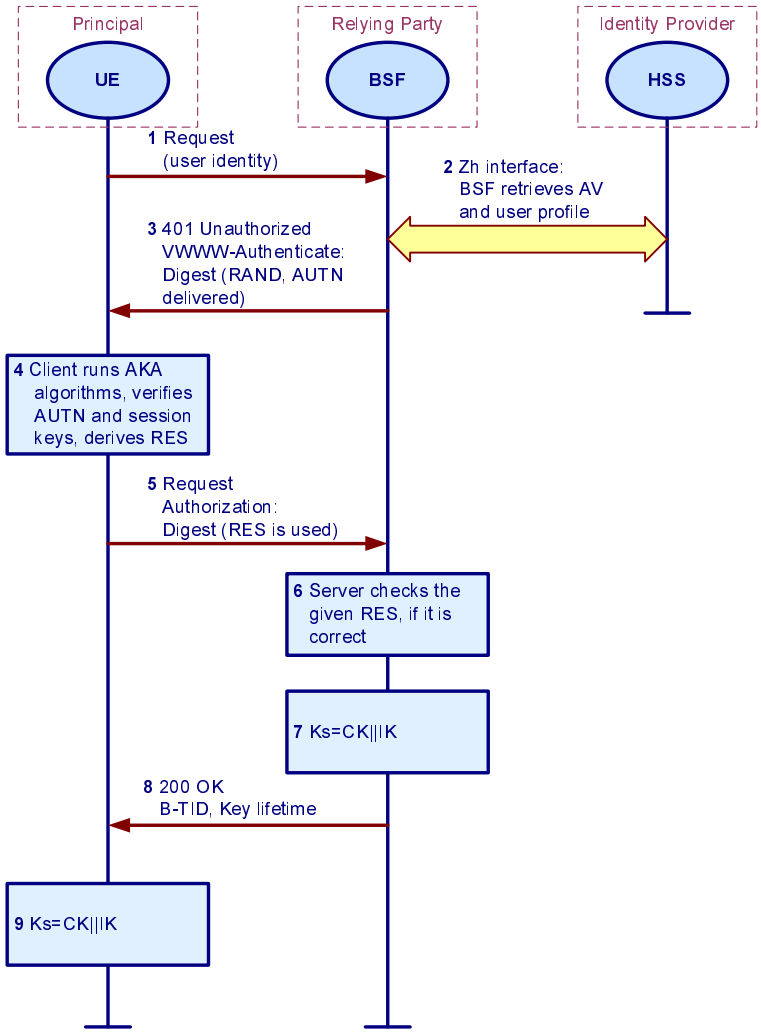



**Figure A.4: The bootstrapping procedure**

After the bootstrapping has completed, the UE and a NAF can run some application specific protocol where the authentication of messages will be based on those session keys generated during the mutual authentication between the UE and the BSF(figure A.5). In the most general situation, the UE and the NAF do not yet have the shared key *Ks_(ext/int)_NAF*. In case a bootstrapping procedure has already happened between the UE and the BSF, the UE is able to derive this key but the NAF does not have it. Therefore, the UE gives an indication to the NAF by the inclusion of *B-TID* (Bootstrapping Transaction IDentifier), to allow the NAF to retrieve the correct key from the BSF. The NAF contacts the BSF (at the Zn reference point), includes this *B-TID* and the *NAF-Id*; this allows the BSF to derive the key *Ks_(ext/int)_NAF* applicable for this NAF. The BSF will provide the key *Ks_(ext/int)_NAF* to the NAF. Now, secure communication between the UE and the NAF can be based on this key.

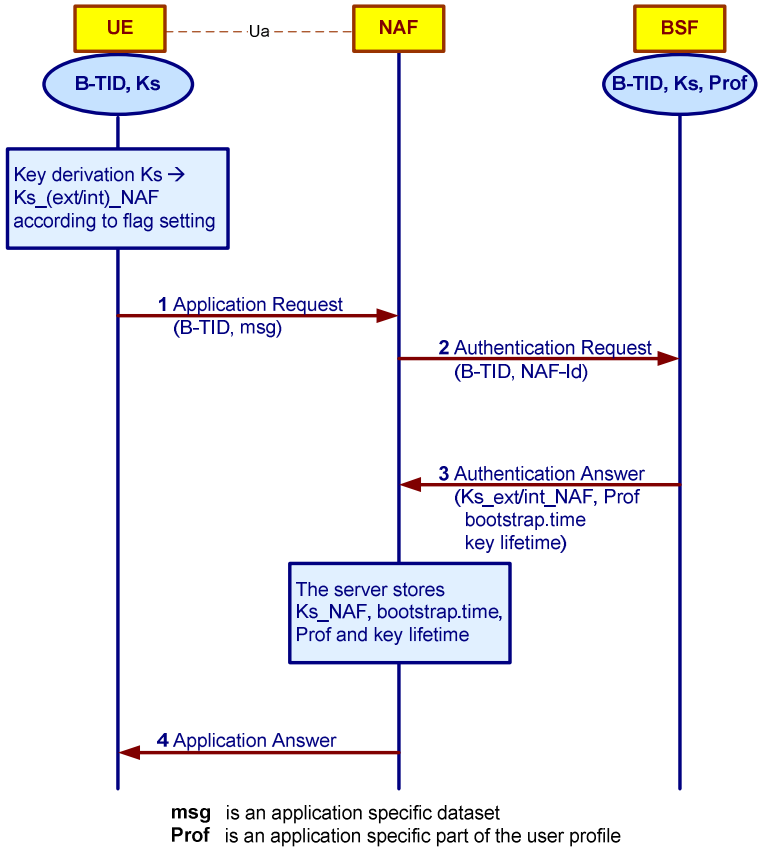



**Figure A.5: The bootstrapping usage procedure**

# A.3 Liberty Alliance Project (LAP)

## A.3.1 Overview

The Liberty Alliance Project (LAP) represents a broad spectrum of industries united to drive a new level of trust, commerce, and communications on the Internet. The members of the Liberty Alliance envision a networked world across which individuals and businesses can engage in virtually any transaction without compromising the privacy and security of vital information.

The LAP specifications actually consist of different modules, as follows:

- The Liberty Identity Federation Framework (ID-FF):
  - specifies core protocols, schemata and concrete profiles for the creation of a standardized identity federation network;
  - enables single-sign-on behaviour on the Internet, for web sites that need user credentials (with minimal active end-user interaction) using a normal Web browser;
  - businesses must affiliate together into "circles of trust" that define the trust relationships between the businesses;
  - users must identify their individual business accounts to their Identity Provider(s) who is then able to indicate that the end-user is authenticated by the Identity Provider (and how he is authenticated), for the different federated businesses.

- The Liberty Identity Web Services Framework (ID-WSF):
  - a set of schemata, protocols and profiles for providing a basic framework of identity services such as identity service discovery and invocation.
- The Liberty Identity Service Interface Specifications (ID-SIS):
  - utilizes the ID-WSF and ID-FF to provide a means of exchanging end-user attribute data in a secure and private controlled manner (i.e. the end-user is able to define what information will be exchanged with other parties).

### A.3.2 Overview of activities

The main goals and achievement of Liberty Alliance are:

- to build open standard-based specifications for federated identity and identity-based Web services;
- to drive global identity theft solutions;
- to provide interoperability testing for products implementing Liberty specifications;
- to offer a formal certification program for products implementing Liberty specifications;
- to establish best practices, rules, liabilities and business guidelines for the implementation of IdM solutions;
- to collaborate with other standards bodies, privacy advocates and government policy groups;
- To address end user privacy and confidentiality issues.

### A.3.3 Current IdM work themes

The Liberty Alliance work programme is divided into several modules as follows:

- the Liberty Identity Federation Framework (ID-FF):
  - specifies core protocols, schemata and concrete profiles that allow identity federation between different businesses;
  - this work has been concluded.
- the Liberty Identity Web Services Framework (ID-WSF):
  - defines a set of schemata, protocols and profiles for providing a basic framework of identity services such as an Authentication Service, a Single Sign-On service, and Identity Mapping Service, an identity-based service discovery service, an identity-based Invocation Service and a People Service;
  - work is also under way to define ID-WSF Advanced Client specifications.
- the Liberty Identity Services Interface Specifications (ID-SIS):
  - specifies network identity services or attribute services (providing additional attribute information about an identity) and utilize ID-WSF and ID-FF specifications. This includes a Personal Profile Service specification, an Employee Profile Service specification and a Contact Book Service specification;
  - work is also being done on a Geolocation Service specification and a Presence Service specification.

### A.3.4 Identities and identifiers used in LAP

Identity information is exchanged between a user agent and the Identity Provider. However, the mechanisms will differ depending upon whether a plain web browser is used (ID-FF) or whether a Liberty enabled client is used (in this case, the authentication service as specified in ID-WSF will be used).

ID-FF specifies single-sign-on scenarios in which identifiers are exchanged between the Identity Provider and the relying service provider. In order to be able to use SSO, the end-user must be authenticated or must already be authenticated by the Identity Provider.

The ID-FF identifiers exchanged between the Identity Provider and the relying service provider (in a SAML assertion) can be any of the following types:

- Federated identifiers:
  - used when a user's identity has been associated at the service provider with the user's identity at the Identity Provider.
- One-time identifiers:
  - used for identifiers with anonymous, single-use semantics exchanged.
- Encrypted identifiers:
  - used for identifiers that have been encrypted for use only be a specific service provider.
- Entity identifier:
  - used for identifiers that identify a Liberty provider or affiliation group.

ID-WSF requires that a web service consumer (WSC) must first be authenticated by an Authentication Service before it can start consuming identity-based services provided by web service providers (WSP).

## A.4 OASIS

### A.4.1 Overview

The work of the following OASIS committees is of particular relevance to IdM. These are:

- the OASIS Security Services Technical Committee which is responsible for the Security Assertion Markup Language (SAML);
- the OASIS Web Services Federation (WSFED) Technical Committee which is currently defining the Web Services Federation Language based on a document previously published within W3C;
- the OASIS Web Services Secure Exchange (WS-SX) Technical Committee which is responsible for the WS-Trust specification;
- the OASIS Extensible Resource Identifier (XRI) Technical Committee which is responsible for defining an extensible, location-independent , application-independent and transport-independent identification scheme that provides addressability not just of resources but also of their attributes and versions;
- the OASIS Identity and Trusted Infrastructure (IDtrust) Member Section which promotes greater understanding and adoption of standards-based identity and trusted infrastructure technologies, policies and practices. The group provides a neutral setting where government agencies, companies, research institutes, and individuals work together to advance the use of trusted infrastructures.

## A.4.2 Identity Management based on WS-Trust and WS-Federation

Figure A.6 shows that OASIS WS-based Identity Management is mainly realized by using the WS-Trust and WS-Federation specification (WS-Federation is still in draft form, while WS-Trust has become an official OASIS standard in March 2007). It also indicates how these two specification fit in the overall WS-Security and Policy protocol stack.

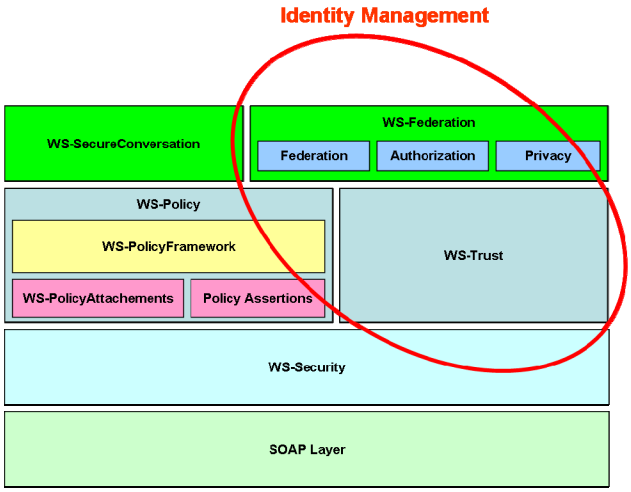



**Figure A.6: OASIS WS-based Identity Management related to the WS Security protocol stack**

While WS-Security defines the basic mechanisms for providing secure messaging, it does not say anything about how to obtain the security tokens necessary to secure web service communications. WS-Trust uses the base mechanisms of WS-Security and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. WS-Trust defines extensions to WS-Security that provide:

- methods for issuing, renewing and validating security tokens by a party that is called a Security Token Service (STS);
- ways to establish and assess the presence of and broker trust relationships.

The Web service security model defined in WS-Trust is based on a process in which a Web service can require that an incoming message prove a set of claims (e.g. name, key, permission, capability). If a message arrives without having the required proof of claims, the service will ignore or reject the message. A service can indicate its required claims and related information in its policy as specified by WS-Policy and WS-PolicyAttachment.

If the requestor does not have the necessary token(s) to prove required claims to a service, it can contact appropriate authorities (as indicated in the service's policy) and request the needed tokens with the proper claims. Within WS-Trust, these authorities are called Security Token Services (STS) (see figure A.7). The Security Token Service as specified in WS-Trust should support token issuance, token renewal and token cancellation.

This general security model – claims, policies, and security tokens – subsumes and supports several more specific models such as identity-based authorization, access control lists, and capabilities-based authorization. It allows use of existing technologies such as X.509 public-key certificates, XML-based tokens, Kerberos shared-secret tickets, and even password digests. The general model in combination with the WS-Security and WS-Policy primitives is sufficient to construct higher-level key exchange, authentication, policy-based access control, auditing, and complex trust relationships.

In summary, Web Services have a policy applied to them. They receive messages from requestors that include security tokens, and have some protection applied using WS-Security mechanisms. The following key steps are performed by the trust engine of a Web Service:

- verify that the claims in the token are sufficient to comply with the policy and that the message conforms to the policy;
- verify that the attributes of the claimant are proven by signatures;

- verify that the issuers of the security tokens are trusted to issue the claims they have made.

If these conditions are met and the requestor is authorized to perform the operation then the service can process the service request.

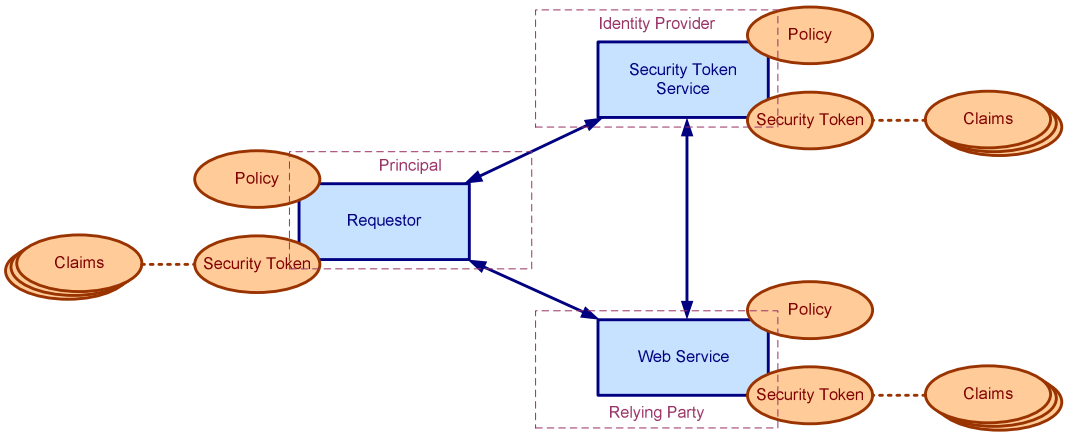



**Figure A.7: Web Services Trust Model**

# A.5 OpenID

## A.5.1 Overview of activities

OpenID is an open source framework of specifications for simplifying user access to restricted web sites. The small set of OpenID specifications is administered by the OpenID Foundation whose primary aim is to provide a decentralized single sign-on mechanism for access to multiple, unrelated web sites. Within such a system, web users do not need to remember traditional authentication tokens such as username and password. Instead, they only need to be previously registered on a website with an OpenID "identity provider", sometimes called an i-broker. Since OpenID is decentralized, any website can employ OpenID software as a way for users to sign in; OpenID solves the problem without relying on any centralized website to confirm digital identity.

## A.5.2 Current IdM work themes

The aspects of IdM which are fundamental to OpenID are:

- user authentication based on a user-supplied identifier;
- a user authenticated at one OpenID-enabled site can move to other OpenID-enabled sites without the need for further sign-on procedures;
- simple transfer of user identity profiles between OpenID-enabled sites;
- the use of a URL as a means of identifying a user.

## A.5.3 Identities or identifiers used in OpenID

Authentication introduces two types of identifiers that can be used with OpenID:

- URLs;
- XRIs (Extensible Resource Identifiers).

### A.5.4 Security of OpenID

OpenID does not have very strong security and can give a false feeling of safety to the user. Its security properties are summarized as follows:

- the user's identity provider is able to track all websites logged into;
- the user has a unique identifier (the OpenID URI) for all relying parties so it is not possible to choose between different identities for different sites. This problem can be circumvented by using multiple IDs but this returns the user to the problem of managing these identities which OpenID was intended to overcome in the first place;
- it is relatively easy to perform phishing attacks on an OpenID identity. Eavesdropping on the identity tokens is also reasonably simple the use of an HTTPS secured connections between the different parties involved in OpenID transactions is not mandated.

# History

| Document history | | |
|---|---|---|
| V2.1.1 | July 2008 | Publication |
| | | |
| | | |
| | | |
| | | |