IDWG Glossary

Important note: footnotes are for information only.

List of entries

(Digital) Identity

A set of representations (data) which one entity communicates to another for the purpose(s) of identification, authentication, authorization or traceability.[1]

The entity can be a person, a legal entity (e.g., a corporation) or an object (e.g., a machine or piece of code).

Note: In the late 19th century, Condorcet, a French mathematician and politician, defined the "identity" as the basis of the contract (contrat social) between an individual and the state.

Unambiguous (or unique) Identity

Unambiguous representations or unique combinations of "Identity elements" .

Identity which is unique in the context(s), where it is used.

Identifier

An identifier is label data (or a bit tag linked to the label data) used to describe an Identity—perhaps, some unique elements in correspondence with an Identity. [2]

Unique Identifier

Label data or a bit tag uniquely linked to the label data for the unambiguous identification of an entity from other or similar entities in a given context.

In some instances, an identifier may be (mis) taken as a signifier for an identity:

Notes:

There is need for a unique and unmodifiable link between the data and the Identity Label.

An identifier is a "pointer" to an identity (or a "profile"). In an analogue universe of paper, pen and forms, identifier elements are name, social security number, tax number, username, IP-address.

In the electronic universe, a link, usually an electronically generated digital signature is used to 'get back' to the Identity.

In this group, we are dealing with the exchange of information between companies, between companies and banks, between companies and public body where payments are involved.

[1] *Alternatives or previous versions*

A set of representations which one entity communicates to another for the purpose(s) surrounding (of?) Identification

An identity is the set of properties of an entity that allows the entity to be distinguished from other similar entities.

A set of elements, which will enable a relying party to recognize a physical person or a legal entity and to differentiate it from another similar entity. It is often synonymous to "identifier".

A set of properties—perhaps, not individually unique to an entity—used in building Identification credentials.

[2] *An identifier is a set of data elements that distinguish an identity from other identities. Therefore, an identifier is a signifier for an identity. Examples of identifiers are name, social security number, tax number, username, IP-address.*

An identifier is label data or a bit tag linked to the label data used to describe an Identity—perhaps, some unique elements in correspondence with an Identity.

A character or a group of characters used to identify or to designate data and, possibly, to specify some of its properties (ISO 2382/IV).

The exchange may take place between two persons, between a person and an application, or between two applications.

Our recommendation is to deal separately with identities of professionals (physical persons) from identities of legal entities, machines, as the issue of "professional identities" is most likely more complex to be solved.

There are many types of identities[3] (or identifiers[4]). Here we restrict ourselves to professional identities, i.e. to identities which relate to a person professional role, activity etc. in a business entity or a public body.

Digital certificates issued by a company to its employees for access control to internal information or issued by the Company's bank for access to banking services are examples of such professional identity.

Credentials

Properties or identifiers?[5].

Identification

1.The process by which an identity is given and registered;

Note: *This is more appropriately designated by "enrolment and registration"(or "provisioning").*

2.The process by which an entity is "identified", that is distinguished from similar or other entities or its "properties, attributes, rights, credentials, exposed (or visualized)..

Note: At some level, it provides an answer to questions like "who is he or she?" for a person, "which company?" or "which object is it?"[6]

[3] *(1) An identity is a set of information that is attributable to a given* **entity**. *[Source:* **Wikipedia on Digital Identity**.*] (2) Identity is a presentation or* **role** *of an* **entity**. *[Source:* **Roger Clarke**.*] (3) a set of claims made by one* **entity** *about itself or another* **entity**. *[Source:* **Kim Cameron**.*] (4) An identity is the set of the properties of an* **entity** *that allows the* **entity** *to be distinguished from other* **entities**. *Identities are owned by their* **entities**. *Identities have several key attributes, including:* **anonymity**, **strength**, *owning* **entity**. *(R)*

[4] *(1) An identifier is information that names or indicates an* **entity** *or* **grouping** *of* **entities**. *[Source:* **Stefan Brands**.*] (2) An identifier is a signifier for an* **identity** *; it is one or more data items that distinguishes an* **identity** *from other identities. Examples of identifiers: name, id-number, username, IP-address. [Source:* **Roger Clarke**.*] (R.)*

[5] *However the word "credential" or "credentials" also designate the actual support bearing the information, like a smart card or a passport with a travel visa: "please give me your credentials".*

[6] *We said initially*

(a) it is the process by which an identity is given and registered, (b) the "visualization" of an identity. An identity may or may not be "authenticated".

(1) Identification is the process whereby data is associated with a particular **identity**. *It is performed by acquiring an* **identifier**. *[Source:* **Roger Clarke**.*] (2) Within a designated* **context**, **identifiers** *enable relying parties to distinguish between the* **entities** *they* **interact** *with. This is known as* **identification**. *[Source:* **Stefan Brands**.*] (3) Identification is the act of claiming an identity, where an identity is a set of one or more signs signifying a distinct entity. [Source:* **Stephen Downes**.*] [See also:* **Authentication**.*] (R.)*

Question: Is electronic identification actually comprised of identification & authentication?

Authenticity

The property that the claimed data source can be verified to the satisfaction of the recipient.

Note: this is more precisely qualified as the “Authenticity of the Origin”

Source : ITU T.411 (93), 3.8

The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information.

Source : ITU J.160 (02), II.1.5 [7]

Integrity

a)The property that data has not been altered or destroyed in an unauthorized manner.

b)The ability of a function to withstand being usurped for unauthorized use, or modified to yield unauthorized results.

Source : ITU Y.140.1 (04), 3.5

Static non modifiable document

An electronic document drafted in such a way that its content is not modifiable during the access and storage phases, as well as is immutable in the time.

Note: to this purpose the electronic document shall not have macro instructions or executable code, capable to activate functions that can modify acts, deeds or data represented in the same document.

Comment: like the ‘totally secure facility’—envisioned yet not very obtainable. Too many unmanaged security layers in commercial systems for an assertion of ‘non-modifiable’ (screen) representation. Storage a difficulty if we are talking of XML forms?

Authentication

Authentication is a process that will enable a relying party to verify two things:

1.The identity assertions offered by an entity (or the claim on an identity). For example that a person or a process is the stated person or process.

2.The validity (or authenticity) of the object, data etc. offered by an entity, to confirm that the entity is the legitimate originator of it. [8]

Note: European law /regulation states that the “authenticity of the origin” and “integrity” of the contents of “electronic interchange” are guaranteed:

[7] *Alternative*

It is the ability of the recipient to qualify the property’s validity by verification (and corroboration) that allows for authentication of the representations

[8] *Alternative*

Authentication is a process that will enable a relying party to verify two things:

1. *the identity of an entity*
2. *the authority of an entity*

The mechanism that verifies that a person or a process is the stated person or process.

- By means of an advanced electronic signature (AES). Member States may however ask for the advanced electronic signature to be based on a qualified certificate,
- or by means of electronic data interchange (EDI) as defined in Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects (See annex 7.3 for the recommendation);
- Invoices may, however, be sent by other electronic means subject to acceptance by the Member State(s) concerned.

[9] A process, which will enable a relying party to actually verify a claim about the “identity” of a person or of an other entity, including the ability of the person to perform specific tasks or activities.

Briefly stated, identification is communicating one’s identity, authentication is bringing supporting elements to the proof of this identity. [from D 530]

Authority

-The right[10] of an entity to perform specific activities, or

-The representations of one entity about another, specific to its rights or allowances in activities (or operations).

Notes: This is subject to the validity recognized by the recipient’s community (of interest) , “entitlement“. [11]

The meaning of authority is slightly different in a wording like “certification authority”.

Authorization

1. he process by which the authority of an entity is defined by the originating party (Syn: habilitation, delegation), or

2. or,he process by which the representation of an authority is granted the permission(s) to engage in (performing) the activities specified under (or covered by) a known (authentified?) authority (loosely the process of entitlement) [12]

[9] *The process of verifying the identity of a user, device, or other entity in a computer system, often as a prerequisite to granting access to resources in a system. A recipient of an authenticated message can be certain of the message's origin (its sender). Authentication is presumed to preclude the possibility that another party has impersonated the sender. (O.)*

Authentication is the process of confirming a system entity’s asserted identity with a specified, or understood, level of confidence [TrustInCyberspace]. (L.A.)

[10] *Synonyms to right: role, habilitation etc.*

[11] *Authority refers to the right of an entity to perform specific activities.*

Authority may refer to the representations of one entity about another, specific to its rights or allowances in activities (or operations). This is subject to the validity recognized by the recipient’s community (of interest) an entitlement.

Synonyms to right: role, habilitation etc.

NB The meaning is slightly different in a wording like “certification authority”.

[12] *Alternatives*

Note: there is a difference between static and dynamic authorizations and grants (entitlements), one which so often becomes problematic in commercial exchanges.

Relying Party

A relying party is an entity that will rely on the identity and authority (NB representations-RPs) of an entity to allow it to perform certain activities (e.g., access to services).[13]

Note: Under appropriate conditions with controlled environments RPs can evaluate products or the services it receives.

Globally, Relying Parties demand to make their own business decisions or judgements, commensurate with their risk. Some Risk Mitigations, like the trust service provision, and the liability bearing framework of it is operating under may be of concern to the RP.

Interchange

Communications between parties take place through interchanges. An interchange is a structure to facilitate (secure) the transfer of one or more messages (e.g. invoices) at one and the same occasion.

Note: Each interchange is designated a unique interchange control reference by the sender. The precise provisions for the designation of references are to be agreed by the parties. The interchange control reference is stated both in the beginning and at the end of the interchange.

Additionally, each interchange has an interchange control count for verification of the number of messages in the interchange.

(a) a process defining what a person is actually able to do, such as access to a specific type of information or to perform a specific operation ("habilitation" in French), (b) the process by which actual permission will be granted to the owner of a right ("authorisation" in French).

Permission given to a user, program, or process to access an object or set of objects. In a modern computer application, authorization is done through the role mechanism. A single person or a group of people can be granted a role or a group of roles. A role, in turn, can be granted other roles. The set of priveleges available to an authenticated entity. (O.)

The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access [SAMLGloss]. (L.A.)

The granting of permission on the basis of authenticated identification. H.235 (03), 3.3 (ITU)

The act of determining if a particular privilege, such as access to telecommunications resource, can be granted to the presenter of a particular credential. J.260 (05), 3.3; Y.1271 (04), 4.3 (ITU)

[13] *Alternative*

A relying party is an entity that relies on the representations made by using an Identifier. How the RP assesses integrity and authenticity of an Identity and Identifier may be via—visualization, out-of-band communication, or electronic computation.

Electronic & Digital Signatures

Digital signature

Data appended to or a cryptographic transformation of, a data unit that allows a recipient of the data to prove the source and integrity of the data unit and protect against forgery (ISO/IEC 7498-2)[14]

Electronic Signature

Data in electronic form that are attached to or logically associated with other electronic data and which serve as a method of authentication (Directive 1999/93/EC)

Advanced electronic signature

An electronic signature, which meets the following requirements:

-it is uniquely linked to the signatory;

-it is capable of identifying the signatory;

-it is created using means that the signatory can maintain under his sole control; and

-it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

(Definition taken from the Directive 1999/93/EC)

Qualified Electronic Signature

An advanced electronic signature based on a “qualified certificate” and created by a secure signature-creation device.

Digital Certificate

A set of ()data issued by an authority or trusted third party.

Note, Together with security information which is used to provide the integrity and data origin authentication services for the data (ITU-T Rec. X.810). *In this Recommendation, the term refers to "public key" certificates which are values that represent an owner's public key (and other optional information) as verified and signed by a trusted authority in an unforgeable format.*

Source : ITU H.235 (03), 3.5

Qualified Certificate

A certificate which meets the requirements laid down in Annex I in the Directive 1999/93/EC and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II.

Certificate Policy

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements (ISO/IEC 9594-8:2001) [5]

Note: a CP may be assigned a unique Object Identifier – ID by an authorised entity.

Certification authority

a body entrusted to create and assign (public key) certificates.

Grace period

Time period which permits the certificate revocation information to propagate through the revocation process to relying parties (ETSI TS 101 733)

[14] *Digital Signatures do not protect against forgery. Nor do they necessarily provide protection of the source.*

Security Policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources (RFC 2828?) .[15]

Electronic Security Policy

The electronically asserted rules which regulate how a system provides security services to protect sensitive and critical system resources.

Time Stamping

Establishing evidence that a datum existed before (at?) that time.

Time Stamping Authority

An authority, which performs time-stamping.

Time Stamp Token

A data object that binds a representation of a datum to a particular time.

Interoperability

An identity is interoperable If:

1. it can be read and interpreted by the (relying) party who receives it (technical interoperability).

   It does not prejudge of what the receiving party will do with it, that is if it will (entitle) authorize the identified entity to use its services. This relying party may be "outside" the "jurisdiction" of the party that issued the identity and authority,

2. The relying party will authorise (entitle) the identified entity to engage in the requested activities (full operational interoperability).

Note: Technical interoperability is a prerequisite for full operational interoperability. This technical view may define the core of interoperability.

There are "views" of interoperability[16], which we might actually qualify with other words like portability, multi-acceptance etc.

[15] *Alternative*

The interpreted set of rules which are applied to specify or regulate how an organization provides security services to protect sensitive and critical system resources (RFC 2828?)

[16] *The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged. ITU Y.101 (00), 35*

The reception and presentation of applications in a vendor-, author- and broadcaster-neutral framework. ITU J.200 (01), 3.1.90

The ability of network management products and services from different suppliers to work together to manage communications between managed object classes". ITU M.60 (93), 2088

The ability for a certificate to enable functions in relationship with applications coming from different organizations and whoever is the certificate originator. (Ref. doc. Groupe des 5).

The ability for heterogeneous services or components to work together. One basic condition of interoperability to enable communication between these services and components is to use of common languages and protocols.

For example, SOAP or XML protocoles are standardized and enable different services to exchange information according to the same rules and methods.

(Agence de l'administration électronique)

Interoperability of identity implies that the relying party is “outside” the jurisdiction of the party that issued the identity and authority;

Portability

An identity is portable if issued by or on behalf of a party it may be used by another party (in a different environment).[17]

Note: Portability is possible if entity Y trusts the identity issued by entity X. Such trust may originate from a registry or a repository of certificates, based on an evaluation framework shared by entity X and Y. Such registries or repositories are put in place by local governments or business communities.

Beyond the technical interoperability mutual recognition of such registries is a key issue.

Multi-acceptance[18]

The same identity is used along a chain of different applications, possibly across company or community boundaries.

[19]See for example the mutual recognition of certificates ref. doc. Groupe des 5 in France.

(Again) there are many degrees of multi-acceptance, like mutual authentication or digital signature.

Mutual recognition of certificates

The same identity is used along a sequence of different applications across company boundaries(ref. doc. Groupe des 5).

Identity, key, certificates infrastructure

An identity infrastructure is an occurrence of architecture, policies, operational and management activities, hardware and software, that covers the lifecycle of identities, keys, certificates and their consumption.

Identity life cycle

The life cycle of an identity is composed by the processes that relate to the management of that identity (e.g., issuance, maintenance, revocation etc.).

Note: Identification, authentication, authorization are just examples of identity “consumption”. Other examples of consumption will be given.

[17] *Alternative*

Portability of identity is synonymous to interoperability of identity.

[18] *“Mutual recognition of certificates” (Ref. doc Groupe des 5)*

At the start of the KMI , interoperability was seen as between certification authorities. But nowadays, the idea of a global root authority seems to have lost his attractiveness except in a facilitating role.

What counts is for applications to be able to deal with multiple certificates.

Users now understand that it will work in practice only if there are common acceptance policies or rules for their applications.

Autrans 2006 (Tutoriel et Atelier Identifiants & Identités)

[19] *Alternative:*

the identity is Interoperable with various (yet common and consistent) electronic security policies

These processes assume that valid identities are “at hand”, i.e. underlying ID life-cycle management processes. [20]

[20] *Should we add the following:*

European Telecommunications Standards Institute:

an independent, non-profit organization, whose mission is to produce telecommunications standards (www.etsi.org)

Hardware Security Module:

the cryptographic module used to securely store the private key and generate the advanced signature in electronic invoices. It may generate the key pair itself or it may securely import a private key securely generated in a secure environment, e.g. another HSM.

Internet Engineering Task Force:

“The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet”; (http://www.ietf.org/overview.html)

Internet Service Provider:

a company that provides users with direct connection to the Internet via either leased or bought direct connections or dialup telephone connections.

Keyed Hashing for Message Authentication:

a mechanism for message authentication using

cryptographic hash functions.

HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key.(RFC 2104)

Private key:

in an asymmetric public key cryptosystem, that key of an entity's key pair which is known only by that entity

Public key:

(1) the key of a signature key pair used to validate a digital signature or (2) the key of an encryption key pair used to encrypt confidential information. …..

Signature Creation Data:

see “Private key”