International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1252

(04/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Baseline identity management terms and definitions

Recommendation ITU-T X.1252

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	**X.1250–X.1279**
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1252

Baseline identity management terms and definitions

Summary

Recommendation ITU-T X.1252 provides definitions of key terms used in identity management (IdM). The terms are drawn from many sources but all are believed to be in common use in IdM work. This Recommendation is not intended to be a huge compendium of IdM-related terms. Instead, the terms defined here are limited to those considered to constitute a baseline list of the most important and commonly-used IdM-specific terms. This Recommendation includes Annex A that explains the rationale for some of these key terms.

One of the main objectives of this Recommendation is to promote a common understanding of these terms among the groups currently developing (or planning to develop) IdM-related standards. The definitions are constructed so that, as far as possible, they are independent of implementations or specific context and, therefore, should be suitable as baseline definitions for any IdM work. It is acknowledged that, in some instances and contexts, greater detail may be required for a particular term, in which case, elaboration of the baseline definition may be considered.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1252	2010-04-16	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Introduction

Compilation of this list of IdM terms and definitions began in 2007. It has had many iterations, received contributions and comments from many people and been reviewed many times. The terms and definitions are from many sources. Some of these, but by no means all of them, are listed in the Bibliography. In some cases, the original definition was suitable and included, but in many cases it was modified or combined with others resulting in a "best of breed" for a particular term.

Considerable effort has been made to ensure that the definitions convey the same meaning as those in other IdM Recommendations | International Standards. This means that, in some cases, the words may not be identical but the meaning should be the same.

Because a term may be used in a number of different contexts, the definitions are confined to a baseline or simple definition of the term without including alternatives or variations that may occur. If additional detail or clarification is needed, this can be added as required.

The fundamental points from which the definitions are derived are discussed further in Annex A.

Recommendation ITU-T X.1252

Baseline identity management terms and definitions

1 Scope

This Recommendation contains a baseline set of definitions of terms commonly used in identity management (IdM). The definitions provide a basic definition of the term, i.e., they are intended to convey the basic meaning although exceptionally, a note is included when it helps to clarify the definition. The rationale for some of the key terms/definitions is included in Annex A.

NOTE – The use of the term "identity" in this Recommendation relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation of a person.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.501] Recommendation ITU-T X.501 (2005) | ISO/IEC 9594-2:2005, *Information technology – Open Systems Interconnection – The Directory: Models*.

[ITU-T X.800] Recommendation ITU-T X.800 (1991, *Security architecture for Open Systems Interconnection for CCITT applications.*

[ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Overview.*

[ITU-T X.811] Recommendation ITU-T X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Authentication framework.*

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1.*

[ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1.*

[ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*

3 Definitions

This clause is intentionally left blank.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

IdM	Identity Management
IdP	Identity Provider
IdSP	Identity Service Provider
NGN	Next Generation Network
PII	Personally Identifiable information
RP	Relying Party

5 Conventions

This clause is intentionally left blank.

6 Terms and definitions

6.1 access control: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

6.2 address: An identifier for a specific termination point that is used for routing.

6.3 agent: An entity that acts on behalf of another entity.

6.4 alliance: An agreement between two or more independent entities that defines how they relate to each other and how they jointly conduct activities.

6.5 anonymity: A situation where an entity cannot be identified within a set of entities.

NOTE – Anonymity prevents the tracing of entities or their behaviour such as user location, frequency of a service usage, and so on.

6.6 assertion: A statement made by an entity without accompanying evidence of its validity.[1]

6.7 assurance: See authentication assurance and identity assurance.

6.8 assurance level: A level of confidence in the binding between an entity and the presented identity information.

6.9 attribute: Information bound to an entity that specifies a characteristic of the entity.

6.10 attribute type [ITU-T X.501]: A component of an attribute that indicates the class of information given by that attribute.

6.11 attribute value [ITU-T X.501]: A particular instance of the class of information indicated by an attribute type.

6.12 (entity) authentication: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

[1] The terms assertion and claim are agreed to be very similar.

6.13 authentication assurance: The degree of confidence reached in the authentication process that the communication partner is the entity that it claims to be or is expected to be.

NOTE – The confidence is based on the degree of confidence in the binding between the communicating entity and the identity that is presented.

6.14 authorization [ITU-T Y.2720], and [ITU-T X.800]: The granting of rights and, based on these rights, the granting of access.

6.15 binding: An explicit established association, bonding, or tie.

6.16 biometric recognition [b-ISO/IEC CD 2382-37]: Automated recognition of individuals based on observation of behavioural and biological characteristics.

6.17 certificate [ITU-T X.810]: A set of security-relevant data issued by a security authority or a trusted third party, that, together with security information, is used to provide the integrity and data origin authentication services for the data.

6.18 claim [b-OED]: To state as being the case, without being able to give proof.[1]

6.19 claimant [ITU-T Y.2720], and [ITU-T X.811]: An entity that is or represents a principal for the purposes of authentication.

NOTE – A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

6.20 context: An environment with defined boundary conditions in which entities exist and interact.

6.21 credential: A set of data presented as evidence of a claimed identity and/or entitlements.

6.22 delegation: An action that assigns authority, responsibility, or a function to another entity.

6.23 digital identity: A digital representation of the information known about a specific individual, group or organization.

6.24 enrolment: The process of inauguration of an entity into a context.

NOTE 1 – Enrolment may include verification of the entity's identity and establishment of a contextual identity.

NOTE 2 – Also, enrolment is a pre-requisite to registration. In many cases, the latter is used to describe both processes.

6.25 entity: Something that has separate and distinct existence and that can be identified in context.

NOTE – An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these entities. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

6.26 entity authentication: A process to achieve sufficient confidence in the binding between the entity and the presented identity.

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

6.27 federation: An association of users, service providers, and identity service providers.

6.28 identification: The process of recognizing an entity by contextual characteristics.

6.29 identifier: One or more attributes used to identify an entity within a context.

6.30 identity: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

NOTE – Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.

6.31 identity assurance: The degree of confidence in the process of identity validation and verification used to establish the identity of the entity to which the credential was issued, and the degree of confidence that the entity that uses the credential is that entity or the entity to which the credential was issued or assigned.

6.32 identity-based security policy [ITU-T X.800]: A security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed.

6.33 identity service bridge provider: An identity service provider that acts as a trusted intermediary among other identity service providers.

6.34 identity management [ITU-T Y.2720]: A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for assurance of identity information (e.g., identifiers, credentials, attributes); assurance of the identity of an entity and supporting business and security applications.

6.35 identity pattern: A structured expression of attributes of an entity (e.g., the behaviour of an entity) that could be used in some identification processes.

6.36 identity proofing: A process which validates and verifies sufficient information to confirm the claimed identity of the entity.

6.37 identity provider (IdP): See identity service provider (IdSP).

6.38 identity service provider (IdSP): An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

6.39 identity verification: The process of confirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information.

6.40 manifestation: An observed or discovered (i.e., not self-asserted) representation of an entity. (Compare with assertion.)

6.41 mutual authentication: A process by which two entities (e.g., a client and a server) authenticate each other such that each is assured of the other's identity.

6.42 name: An expression by which an entity is known addressed or referred to.

NOTE – A name is used within a context and cannot be assumed to be unique or unambiguous. For routing purposes, it may be resolved or translated into an address.

6.43 non-repudiation: The ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action.

6.44 pattern: See identity pattern.

6.45 persistent: Existing and able to be used in services outside the direct control of the issuing assigner, without a stated time-limit.

6.46 personally identifiable information (PII): Any information a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains; b) from which identification or contact information of an individual person can be derived; or c) that is or can be linked to a natural person directly or indirectly.

6.47 principal [ITU-T Y.2720], [ITU-T X.811], and [ITU-T Y.2702]: An entity whose identity can be authenticated.

6.48 privacy: The right of individuals to control or influence what personal information related to them may be collected, managed, retained, accessed, and used or distributed.

6.49 privacy policy: A policy that defines the requirements for protecting access to, and dissemination of, personally identifiable information (PII) and the rights of individuals with respect to how their personal information is used.

6.50 privilege: A right that, when granted to an entity, permits the entity to perform an action.

6.51 proofing: The verification and validation of information when enrolling new entities into identity systems.

6.52 pseudonym: An identifier whose binding to an entity is not known or is known to only a limited extent, within the context in which it is used.

NOTE – A pseudonym can be used to avoid or reduce privacy risks associated with the use of identifier bindings which may reveal the identity of the entity.

6.53 registration: A process in which an entity requests and is assigned privileges to use a service or resource.

NOTE – Enrolment is a pre-requisite to registration. Enrolment and registration functions may be combined or separate.

6.54 relying party (RP) [ITU-T Y.2720]: An entity that relies on an identity representation or claim by a requesting/asserting entity within some request context.

6.55 repudiation: Denial in having participated in all or part of an action by one of the entities involved.

6.56 requesting entity: An entity making an identity representation or claim to a relying party within some request context.

6.57 revocation: The annulment by someone having the authority, of something previously done.

6.58 role: A set of properties or attributes that describe the capabilities or the functions performed by an entity.

NOTE – Each entity can have/play many roles. Capabilities may be inherent or assigned.

6.59 security audit [ITU-T X.800]: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

6.60 security domain [ITU-T Y.2720], [ITU-T Y.2701], and [ITU-T X.810]: A set of elements, a security policy, a security authority, and a set of security-relevant activities in which the elements are managed in accordance with the security policy.

6.61 security zone [ITU-T Y.2701]: A protected area defined by operational control, location, and connectivity to other device/network elements.

6.62 security domain authority [ITU-T X.810]: A security authority that is responsible for the implementation of a security policy for a security domain.

6.63 **self-asserted identity**: An identity that an entity declares to be its own.

6.64 **trust**: The firm belief in the reliability and truth of information or in the ability and disposition of an entity to act appropriately, within a specified context.

6.65 **trust level**: A consistent, quantifiable measure of reliance on the character, ability, strength, or truth of someone or something.

6.66 **trusted third party** [ITU-T Y.2702], [ITU-T X.800], and [ITU-T X.810]: In the context of a security policy, a security authority or its agent that is trusted with respect to some security relevant-activities.

6.67 **user**: Any entity that makes use of a resource, e.g., system, equipment, terminal, process, application, or corporate network.

6.68 **user-centric**: An identity management (IdM) system that provides the user with the ability to control and enforce various privacy and security policies governing the exchange of identity information, including the users' personally identifiable information (PII), between entities.

6.69 **verification**: The process or instance of establishing the authenticity of something.

NOTE – Verification of (identity) information may encompass examination with respect to validity, correct source, original, (unaltered), correctness, binding to the entity, etc.

6.70 **verifier**: An entity that verifies and validates identity information.

Annex A

Key points and rationale for IdM basic terminology

(This annex forms an integral part of this Recommendation)

Background

Discussions on identity management (IdM) have illustrated differences in the understanding that people have about the intention of IdM, about the basic procedures used, and in the terminology and definitions of terms. These differences have led to misunderstandings and lengthy discussions during the IdM standardization process.

To help avoid these misunderstandings in the future, this annex captures some of the agreements reached during ITU-T discussions on these basic concepts and terminology and helps explain the thinking that went into the development (or, in some cases adoption) of the terms included in this Recommendation. Please note that this annex does not capture or explain the holistic view of identity management.

Introduction

Identity is the term around which all other IdM terms revolve. In the real world, rather than digital world, for example, the identity of a natural person is readily accepted and is based upon an extensive set of characteristics or attributes. Some of these are physical features such as height, hair colour, general appearance, mannerisms, behaviour, etc. Others, like date of birth, place of birth, home address, telephone number may also be used. In a communication process, both parties normally have the requirement to have enough confidence that they communicate with the correct partner. This process of seeking this confidence would often involve two or more individuals or "entities": the entity whose identity is to be confirmed – the *requesting entity,* and the entity that will rely on a confirmed identity – the *relying party*. A third entity which manages identities may be involved – an *identity service provider.*

In the digital or "on-line" world, an "identity" is also made up of attributes, just like the real world. However, in this case, the "identity" may be limited to a single feature or it may have many; it will depend on the context in which it appears. This applies to inanimate objects as well as natural persons so users are often referred to as an entity.

Generally, identifiers, and/or attributes will uniquely characterize an entity within a particular context. Because of this, an entity may have a number of different identities some of which will be a subset of other identities.

A.1 Authentication and confidence

The authentication process is a major part of IdM. The following is provided to help explain the authentication process and its relevance to confidence.

Note that, when applying this model to real procedures and applications, one has to be very clear about the relevant communication partners and the applicable chains of trust.

The authentication process may be described as follows:

Most communication processes require that the communication partners have adequate confidence or trust that they are really communicating with the intended partner. Therefore, at the beginning of a communication, the partners try to reach an adequate level of confidence on the basis of available identity information about the partner, i.e., confidence in the binding between the entity and the presented identity.

The process of establishing confidence is especially important when the communicating partners are remote from each other and connected only by a telecommunication link. The authentication process is executed in order to ascertain, with a sufficient degree of confidence that the identity presented by a communication partner really belongs to it.

Communication always involves two or more distinct partners that exchange information. Due to the broad variety of possible partners (e.g., humans and things), a general term needs to be defined. The term chosen is *entity* which is defined as: something that has separate and distinct existence and that can be identified in context.

NOTE –

- An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, software application, service, etc., or a group of these entities.
- In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

The information that can be used for identification of an entity is based on the entity's attributes. An *attribute* is defined as*:* information bound to an entity that specifies a characteristic of the entity. In practical terms, identification of an entity is usually based on a subset of its attributes since identification is limited by what is called the context, within which the entity exists and interacts. The narrower the context and the clearer the boundary conditions, the fewer the number of attributes necessary for identification. *Context* is defined as: an environment with defined boundary conditions in which entities exist and interact.

Since the definition of entity is based on the capability to be identified, it is necessary to have a proper definition of *identification:* the process of recognizing an entity as it is characterized within a context.

For the purpose of distinguishing entities, it is sufficient to use a sub-set of the attributes which is adequate to the context. This is referred to as the *identity* which is defined as: a representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within a context. For IdM purposes, the term identity is understood as a contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

An identity can be a subset of another identity. There also may be intersections of identities. However, for various reasons (such as for privacy concerns), intersections of identities, used for different purposes or in different contexts, may be explicitly undesirable or even excluded.

Figure A.1 shows the relationships between entity, identities and attributes.

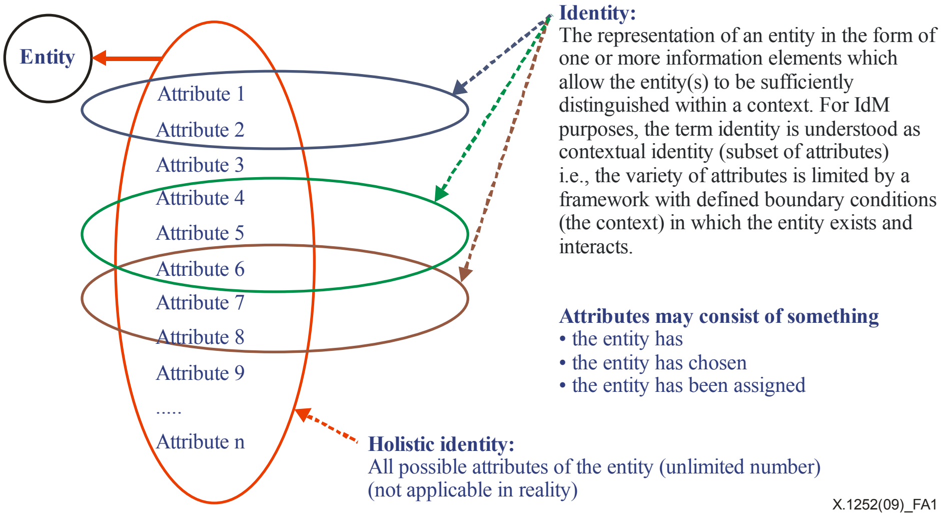

Entity
Attribute 1
Attribute 2
Attribute 3
Attribute 4
Attribute 5
Attribute 6
Attribute 7
Attribute 8
Attribute 9
.....
Attribute n
Identity:
The representation of an entity in the form of one or more information elements which allow the entity(s) to be sufficiently distinguished within a context. For IdM purposes, the term identity is understood as contextual identity (subset of attributes) i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.
Attributes may consist of something
• the entity has
• the entity has chosen
• the entity has been assigned
Holistic identity:
All possible attributes of the entity (unlimited number) (not applicable in reality)
X.1252(09)_FA1

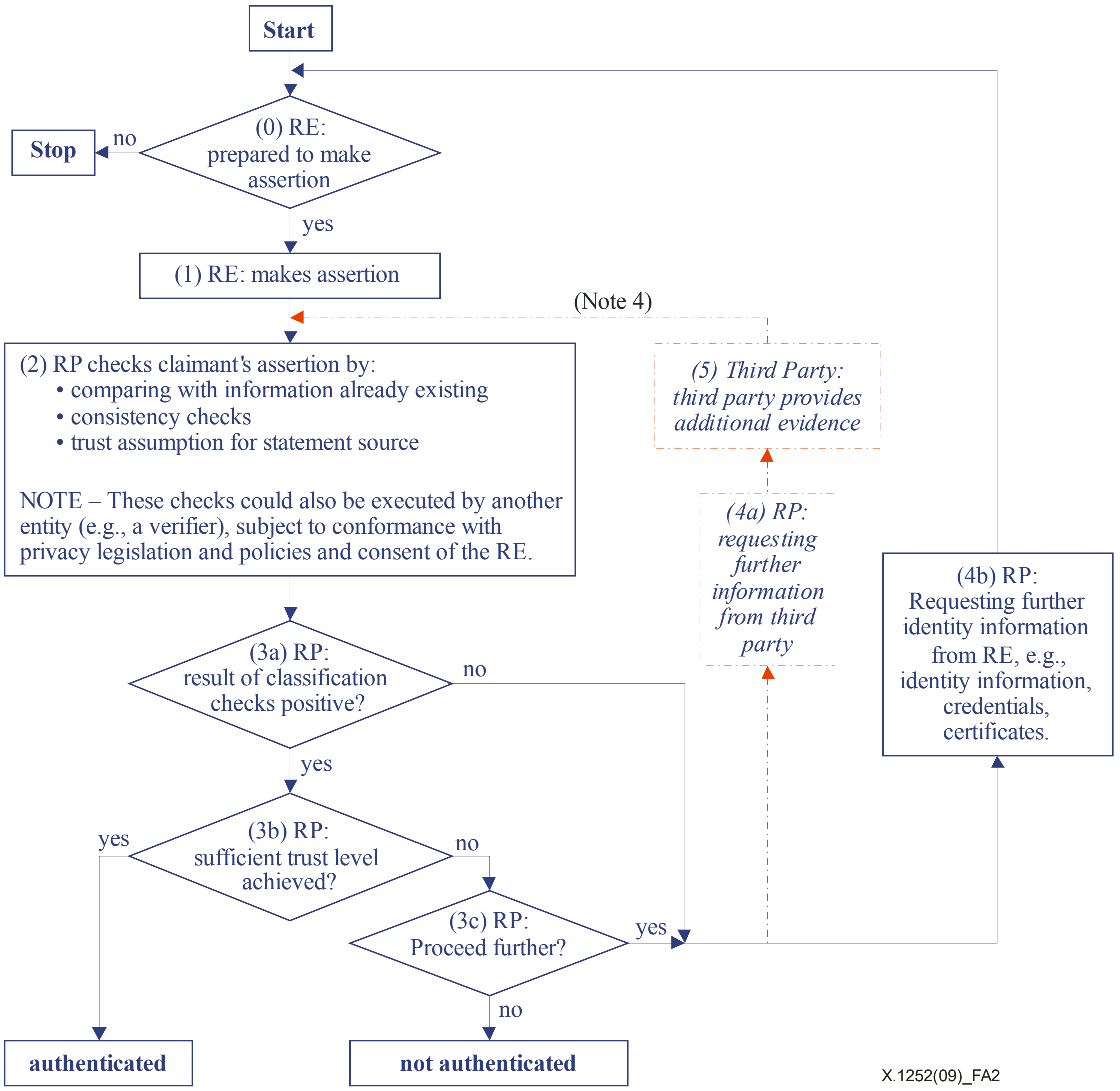
Figure A.1 – Relationships between entity, identities and attributes

As already noted, authentication is relevant for identity management. It is the process needed to achieve sufficient confidence that communication is being undertaken with the intended partner. The actual level of confidence needed will depend on the sensitivity of the application and/or the risk of consequent damage due to engaging in communication with the wrong partner.

Rights or privileges can be assigned for various purposes including, for example:

- sharing or delivering of information which is not intended to be available for everybody;
- granting access to:
  - information;
  - rooms/areas/domains;
  - services;
  - usage of resources;
- making contracts.

Gaining such confidence requires that the communication partner can be clearly distinguished from other possible communication partners and that, when required, this distinction can be periodically reassessed.



NOTE 1 – This figure shows the basic unidirectional authentication process. Generally this process is executed mutually in parallel and/or interleaved.
NOTE 2 – If no trust level is required, step 2 may be dropped.
NOTE 3 – This flow can be executed multiple times, and those recursions also could be separated in time and/or location.
NOTE 4 – Involvement of third party is subject to privacy legislation and policies and consent of RE. (-·-·-·-·-)

Figure A.2 – Unidirectional authentication process

In general this process of achieving confidence, i.e., the authentication process, is done mutually. That means that the authentication process as shown in Figure A.2 is accomplished twice with each of the entities acting in each role, i.e.:

Authentication of Y: Entity Y acts as requesting entity (RE), entity X acts as relying party (RP)

Authentication of X: Entity X acts as requesting entity, Y acts as relying party

For simplification and easier understanding, the authentication process shown in Figure A.2 is described in one direction only. However, the flows of these two processes are interleaved.

Interleaved execution allows the parties to check pre-conditions before presenting potentially confidential attributes. Such conditions can be:

- knowledge of how to address the relying party,
- sufficient trust that the relying party is the right one (e.g., users should have some confidence, that they are on the right web page, before entering identity information such as user name and password).

In some cases (but not in user-centric systems) a third party could be directly involved to provide further information as evidence to the relying party to improve trust in the attributes of the requesting entity.

Identities are comprised of attributes. Those can be something:

- the entity has (e.g., code card)
- the entity knows (e.g., password)
- the entity is (e.g., colour, size)
- the entity is able to do (e.g., specific encryption)
- the location of the entity
- combination of those.

Identities can be checked by:

- consistency of the information itself
- consistency with other supporting information
- comparing with already known information.

Attributes can also be specified in terms of an *identity pattern* which is a structured expression of attributes of an entity (e.g., the behaviour of an entity) that could be used in some identification processes.

Note particularly that, as shown in the Figure A.2 flowchart example, it is always up to the RP to decide whether to accept the requesting entity or not on the basis of the authentication process. No one else can make this decision.

In general, every communication partner should be able to set the level of confidence needed to allow the execution of privileges. However, this right can be limited and, in some cases, has to be limited by legislation.

Where there is a significant asymmetry between the communication partners, there is particular danger that the more powerful partner could misuse this situation and require an insufficiently high level of confidence, or refuse his own authentication. Therefore, it is necessary that technical implementations of authentication mechanisms be based on symmetric mechanisms to avoid asymmetry. In addition, there could be the need for regulations to prevent dominance of one party to prevent undue usage of a dominance situation in asymmetric situations.

In general, when applying identity management, it is necessary to be very clear about the entities involved and their purpose so that the context and identities (set of attributes) can be limited to the specific purpose.

For the level of confidence with respect to pure telecommunications purposes, it is usually sufficient that the customer has appropriate confidence to be connected to the intended transport or service provider and the providers have confidence that the usage of services is permitted, can be billed and should be paid. The latter could be achieved by authentication of, for example, an access point or a subscriber account, which need not be identical with, or reference the actual user of the service. In some cases, such as prepaid phone cards or prepaid SIM-cards, no authentication will be necessary.

A credential may be presented in the authentication process as evidence of some or all attributes of a presented contextual identity. A *credential* is defined as: a set of data presented as evidence of a claimed identity and/or entitlements. However, it is necessary to distinguish clearly between two types of credential:

1) A set of data presented as evidence of a claimed identity, which is relevant for authentication purposes (e.g., a passport). This type of credential is used to increase the trust in attributes by confirmation through the party which issues the credential; and

2) A set of data presented as evidence of entitlements, which is relevant for authorization purposes only (e.g., a ticket for a concert or football game). It allows the exercise of a privilege (such as being admitted to an event on the basis of having a ticket) without necessarily revealing the identity of the entity presenting the credential.

Some credentials may include both functions and both types of credential could be subject to a separate authentication process.

A.2 Claim/assertion

The meaning of the terms claim and assertion are generally agreed to be somewhat similar but with slightly different meanings. In some cases, an assertion is considered to be a "stronger" statement than a claim. For example, the Oxford English Dictionary defines claim as:

a) to state as being the case, without being able to give proof;

b) a statement that something is the case,

and assertion as: a confident and forceful statement. However, in a digital context, the terms "confident" and "forceful" are not really meaningful.

In open networks, there will be a more complex and ambivalent relationship between the party making a statement (i.e., presenting identity information) and the party that relies on it. Therefore, any statement is assumed to be in doubt and, as such, is subject to verification or request for further evidence. Neither claims nor assertions can be assumed to be made with any authority whatever. It will always be up to the relying party to decide whether or not to accept the claim or assertion based on verification by the relying party (or by a verifier acting at the request of the relying party).

A.3 Enrolment and registration

Enrolment and registration are two processes that are closely related and there is overlap between the two. The terms are sometimes used interchangeably and, although they may be combined in a single step, there are, in fact, two distinct processes.

Enrolment is: the process of inauguration (or establishing) of an entity into a context. Enrolment may include verification of the entity's identity and establishment of a contextual identity. Registration is: the process in which an entity requests, and is assigned, privileges to use a service or resource. Enrolment is a pre-requisite to registration.

In the real world, for example, a user may, at some point, enrol for generic banking services, then, at a later time register for on-line banking. Alternatively, the user may, when opening a new account, fulfil identification (and related) formalities (i.e., enrol) and register for on-line banking services at the same time.

A.4 Identity provider and identity service provider

An examination of current practice indicated that the terms *identity provider* and *identity service provider* are both commonly used. Although the term *identity provider* is used in some existing ITU-T Recommendations, it could be construed to mean an entity that *provides* identities, rather than an entity that *manages* identities. Furthermore, this term is misleading because identities cannot be provided, they exist, or evolve when attributes are assigned. In addition, the term *service* *provider* is used quite extensively in terms like verification service provider, credential service provider, financial service provider, etc.

The term i*dentity service provider* is, therefore, seen as somewhat more descriptive than *identity provider* and should be the preferred term. It was possible to accommodate this change with only a minor impact to the existing documents by using the current definition of *identity provider* for *identity service provider* and retaining the term *identity provider* but, instead of defining it, simply providing a pointer to *identity service provider.* The acronym should be IdSP.

A.5 Identity pattern

In general, patterns are regarded as information that is observed or recognized and for which a structure can be detected, or which fits in an already known structure. So an identity pattern may be considered to be information that characterizes an entity which is observed or recognized and for which a structure can be detected or which fits to an already known structure.

For example, two relevant dictionary definitions of the term *pattern* are: "a regular or repetitive form, order or arrangement"; and "a reliable sample of traits, acts, tendencies, or other observable characteristics of a person, group or institution".

The general view and the above definitions of pattern imply that there is more than one element to the pattern but the repetition of a single attribute over time also constitutes a pattern. A single occurrence of a single attribute would not constitute a pattern but the manner of occurrence of one or more attributes can form a pattern. Also, an identity pattern can be based on more than an activity or behaviour and is not limited to information which is observed or recognized. Rather it can be based on any attribute(s). For example, a tyre profile has a clear and detectable structure so, in this case, the attribute itself may be considered an identity pattern. Nor is it necessarily the case that a pattern must be observed more than once to be useful. For example, when two people talk about a car in the showroom of a dealer, they could identify and refer to it as: "The one standing in the rear left corner".

Patterns may be reusable but one could also conceive of situations where the pattern is used only once, such as one-time codes.

Although it may be argued that all attributes have some kind of structure, a clear difference between attributes and identity patterns is that a structure is detected and derived by the observer but the structure is not necessarily known by other entities, even the observed entities.

Identity patterns may be used not only for identification purposes but also, in some instances, for authentication or simply to categorize or classify entities. An example of the latter is where consumer behaviour is scanned to determine which kinds of products they buy and how often they buy such products. In such a "marketing" context, patterns are used to classify entities in relation to certain groups of entities but, combining some of such patterns together, could result in the identification of single entities.

The elements used to identify an entity must allow the entity to be sufficiently distinguished within context. If an identity pattern is going to be used for individual (as opposed to group) identification or authentication, the identity pattern needs to be unique and unambiguous. However, in some instances, e.g., where an identity pattern is used for authorization, it may not need to be unique or unambiguous. An example might be where it is necessary to limit users of a particular service, e.g., participation in sport competitions. There it may be necessary to apply restrictions, e.g., based on behaviour on consumption of certain medicines.

Bibliography

In developing this list of IdM terms and definitions, reference has been made to a large number of IdM publications, work and glossaries that already exist. The list is far from exhaustive but includes:

[b-ISO/IEC CD 2382-37] ISO/IEC CD 2382-37, *Information technology – Vocabulary – Part 37: Harmonized biometric vocabulary*.

[b-ANSI] American National Standards Institute http://www.ansi.org/

[b-AusCert] AusCert Conference 2005

[b-Carnegie] Carnegie Mellon® Computing Services www.cmu.edu/acs/documents/idm/

[b-NSS] Committee on National Security Systems GlossaryWorking Group

[b-Edentity] Edentity http://www.edentity.co.uk/

[b-ETSI] ETSI Terms and Definitions Database Interactive – http://webapp.etsi.org/Teddi/

[b-EU] EU Commission eGovernment Unit DG Information Society and Media

[b-ICANN] ICANN http://www.icann.org/en/general/glossary.htm

[b-Identity] Identity Commons http://wiki.idcommons.net/Main_Page

[b-IETF] IETF Trust (2007) Network Working Group

[b-ISO/IEC] ISO/IEC JTC 1/SC 27/WG5

[b-ITU-T Id Mgmt] ITU-T Identity Management Focus Group

[b-ITU-T Terms] ITU-T Terms and Definitions Database – http://www.itu.int/ITU-T/dbase

[b-Cameron] Kim Cameron's Laws of Identity http://www.identityblog.com/?p=354

[b-Liberty] Liberty Alliance Technical Glossary

[b-Modinis] Modinis https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome

[b-NetMesh] NetMesh® Inc. http://www.netmesh.us/

[b-NIST] National Institute of Standards and Technology http://www.nist.gov/index.html

[b-OASIS] OASIS http://www.oasis-open.org/committees/security/ipr.php

[b-OED] Oxford English Dictionary

[b-OECD] OECD Recommendation on Electronic Authentication

[b-Mobile] Open Mobile Alliance™ http://www.openmobilealliance.org/UseAgreement.html

[b-STORK] STORK-eID Consortium http://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1

[b-Trusted] Trusted Computing Group http://www.trustedcomputinggroup.org/

[b-IAAC] UK Information Advisory Council http://www.iaac.org.uk/Default.aspx?tabid=1

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2010