Report on the Definition of the Term "Identity"

Contents

Summary

The Correspondence Group on the Definition of the Term "Identity" conducted its work over a period of several weeks through a combination of on-line exchange of materials and dialogue, including informal discussion at the IdM GSI, Seoul, January 2008.

This work confirmed that the term "identity" is one that has been used extensively across all ITU, ICT, and security communities for decades if not generations, and is found in nearly one thousand ITU-T and ITU-R standards alone.

It was apparent also that the term "identity" in all these many contexts (i.e., its ontology), is one that exists as an abstraction or concept for countless different kinds of representations of an entity at different points in time and location. These representations take the form of structured credentials, identifiers, attributes, or patterns that are asserted or manifested by an entity – that are captured in many different ways with bindings to the represented entity. The term "identity" is not the same as derivative services such as "identification." Some specific (defined) set of credentials, identifiers, attributes, and patterns may constitute "positive identification," but such instances would have to be agreed and dealt with by the parties - which is out-of-scope.

If it is necessary to describe or define "identity," it is suggested that the following be used.

> **identity**. The assertion or manifestation of a structured representation of an entity in the form of one or more credentials, identifiers, attributes, or patterns. Such representations can take any physical or electro-optical form or syntax, and have associated implicit or explicit time-stamp and location specifications.

This definition is not constrained to any particular communication media or context, and is thus suitable for all uses within the ITU for all ICT implementations, including radio systems.

In addition, because identifiers are one the four possible constituents of identity, the term "identifier" cannot be regarded as a replacement for "identity." It is not also apparent that the term "trusted identifier" has ever been used within the ITU or industry forums.

Similarly, the use of "identity" in the essentially ubiquitous phrase "identity management," can be described or defined as follows.

> **identity management.** The diverse arrays of different technical, operational, and legal systems and practices involving the structured capture, syntactical expression, storage, tagging, retrieval, and destruction of entity identities.

1. Scope

Development of a coherent definition of the terms *identity* and *Identity Management* as they relate to trusted assertions of identity for the purposes of telecommunication/ICT that would be acceptable to all interested parties.

2. References

[1] *See* Results of the Editing Group on text for JCA-IdM and IdM-GSI, TSAG Doc. TD549 Rev. 1, Dec 2007. See also, Germany, Use of the term "Identity" in ITU-T, TSAG Doc. C48, Dec. 2007.

[2] *See* Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations [unofficial version for industry consultation for official German text please refer to the Official Journal (Bundesgesetzblatt – BGBl. Teil I S. 876 vom 21. Mai 2001)]

[3] See, e.g., Technical Report Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456), ETSI TR 102 458 V1.1.1 (2006-04)

3. Definitions

For the purposes of this report, the following definitions are used.

attribute. Information bound to an entity that specifies a characteristic of an entity such as condition, quality, presence, or other information associated with that entity. [Same as the IdM Focus Group definition except for the addition of the word "presence."]

credential. Authentication and Authorization data that can be used to authenticate the claimer is what it claims to be and authorize the claimer's authority. [Same as the IdM Focus Group definition except it replaces "claimer's rights" with "claimer's authority."]

entity. Anything with a describable existence at some location within some timescale. [Differs from the IdM Focus Group definition which is too narrow for the purposes of considering the definition of identity.]

identification services. A service that aggregate an entity's identities to provide trust levels in the bindings among the identities and the entity. [The definition does not exist in the IdM Focus Group reports.]

identifier. An identifier is a series of digits, characters and symbols or any other form of data used to identify subscriber(s), user(s), network element(s), function(s), network entity(ies) providing services/applications, or other entities (e.g., physical or logical objects). [Same as the IdM Focus Group definition.]

identity. The assertion or manifestation of a structured representation of an entity in the form of one or more credentials, identifiers, attributes, or patterns. Such representations can take any physical or electro-optical form or syntax, and have associated implicit or explicit time-stamp and location specifications. [Differs from the IdM Focus Group definition which is too narrow for the purposes of considering the definition of identity.]

identity management. The diverse technical, operational, and legal systems and practices involving the structured capture, syntactical expression, storage, tagging, retrieval, and destruction of entity identities. [Differs from the IdM Focus Group definition which is too narrow for the purposes of considering the definition of identity.]

pattern. A structured expression derived from the behaviour of an entity that contributes to the recognition process; this may include the reputation of the entity.

Identity patterns may be uniquely associated with an entity, or a class with which the entity is associated. [Differs from the IdM Focus Group definition which is too narrow for the purposes of considering the definition of identity.]

presence. A set of attributes that characterize an entity (maintained by a "presentity") such as current activity, environment, geolocation, communication means and contact addresses. [The definition does not exist in the IdM Focus Group reports. Ref. RFC 2778.]

4. Abbreviations and Acronyms

IdM identity management

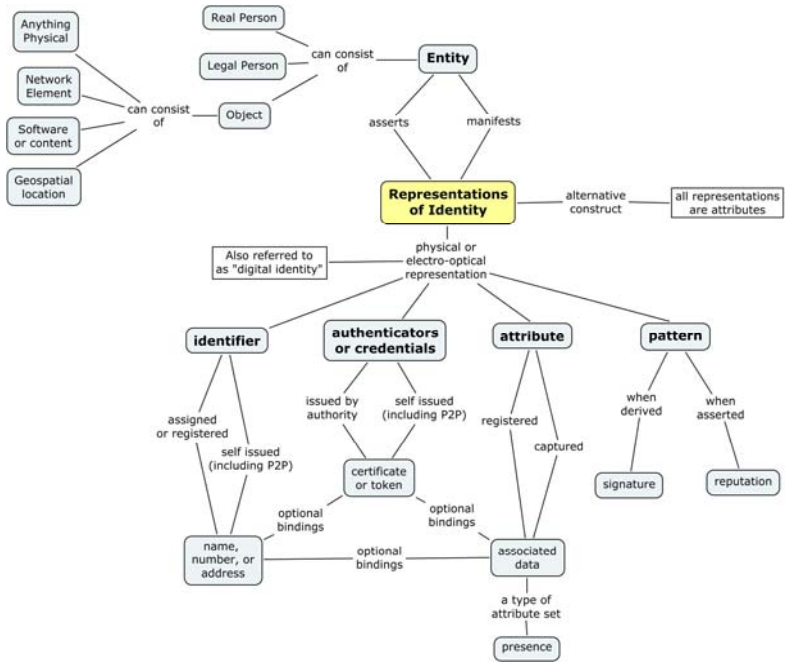
5. Conventions

Not applicable.

6. Executive summary

The work confirmed that the term "identity" is one that has been used extensively across all ITU, ICT, and security communities for decades if not generations, and is found in thousands of contexts in hundreds of ITU-T standards alone.

In proceeding with the work of the basic task of the Correspondence Group to develop a core definition of "identity," plus the related definition of "identity management," the editor developed an Identity Ontology "living" diagram that was discussed and refined over the life of the Group. See below.



This diagram proved a useful means to focus on the definitional objective and was among many hundreds of participants not only on the official ITU-T Correspondence Group list, but also other lists of "identity community" developers and at tutorials and meetings at key ITU-T Identity Management meetings.

This activity revealed that the term “identity” in all the many legacy and contemporary contexts (i.e., its ontology), is one that exists as an abstraction or concept for countless different kinds of representations of an entity at different points in time and location. The term “identity” is rarely if ever used in any absolute sense because it consists of an almost infinite number of representations for every entity. To the extent that some kinds of reliance occurs, it arises from identification services that aggregate an entity’s identities to provide trust levels in the bindings among the identities and the entity.

Identity representations take the form of structured credentials, identifiers, attributes, or patterns that are asserted or manifested by an entity – that are captured in many different ways with bindings to the represented entity. The term “identity” is not the same as derivative services such as “identification.” Some specific (defined) set of credentials, identifiers, attributes, and patterns with some understood assurance level may constitute “positive identification” in some context, but such instances would have to be agreed and dealt with by the parties concerned as a legal matter and is out-of-scope of this work.

If it is necessary to describe or define “identity,” it is suggested that the following be used.

> **identity**. The assertion or manifestation of a structured representation of an entity in the form of one or more credentials, identifiers, attributes, or patterns. Such representations can take any physical or electro-optical form or syntax, and have associated implicit or explicit time-stamp and location specifications.

This definition is not constrained to any particular communication media or context, and is thus suitable for all uses within the ITU for all ICT implementations, including radio systems. In addition, because identifiers are one the four possible constituents of identity, the term “identifier” cannot be regarded as a replacement for “identity.” It is not also apparent that the term “trusted identifier” has ever been used within the ITU or industry forums.

Similarly, the use of “identity” in the essentially ubiquitous phrase “identity management,” can be described or defined as follows.

> **identity management.** The diverse arrays of different technical, operational, and legal systems and practices involving the structured capture, syntactical expression, storage, tagging, retrieval, and destruction of entity identities.

7. Background information

During the course of the Identity Management related meetings over the past eighteen months, some concern has occasionally been raised regarding the use of the term “identity” in the context of Identity Management activities, reports, and standards. At the recent meeting of the Telecommunications Standards Advisory Group (TSAG), this concern resulted in tentative agreement, pending further potential discussion at future TSAG meetings, to include the following note in the terms of reference of the JCA-IdM and IdM-GSI forums:
The use of the term “identity” in this ToR and in the future ITU-T activities relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation. [1]

Subsequent to the TSAG meeting and responsive to the concerns expressed at the TSAG meeting, the Q6/17 Rapporteur Group created a Correspondence Group on the definition of the term “identity.” The Terms of Reference for this group is included as Annex A. At

this meeting, Amardeo Sarma of NEC Laboratories Europe expressed his willingness to serve as Vice-Convenor or this Group and it was understood that he would serve in this capacity.
This document provides an initial baseline contribution for the work of the Correspondence Group.

8. Objective of this document

This document describes the work of the Correspondence Group and provides its deliverables pursuant to its Terms of Reference.

9. Historical use of the term "Identity"

As was noted at the TSAG meeting through TSB staff research, the concept and use of "identity" has been used by the ITU generally and the ITU-T specifically, for many decades, and is found thousands of places in more than a quarter of all the current ITU standards Recommendations – many jointly adopted with ISO/IEC. In work undertaken by the ITU IS department, the term "identity" appears in 828 ITU-T and 112 ITU-R Recommendations. See Annex B.

In the context of what is generally regarded as Identity Management, the ITU-T conceptualized the term "identity" more than twenty years ago, and included its use in fundamental ways in ITU-T Open Systems Interconnection standards that have been widely implemented by industry and governments in infrastructures supporting security, directory, eMail, and network management services. *See, e.g.*, Annex C. However, the term "identity" was apparently never explicitly defined.

Searches uncovered innumerable adoption of the use of "identity" in national digital signature legislation and related standards. [2][3] One of the more prominent national provisions are found in Germany's recent Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations where the term "identity" constitutes the basis for the legislative action. [2]

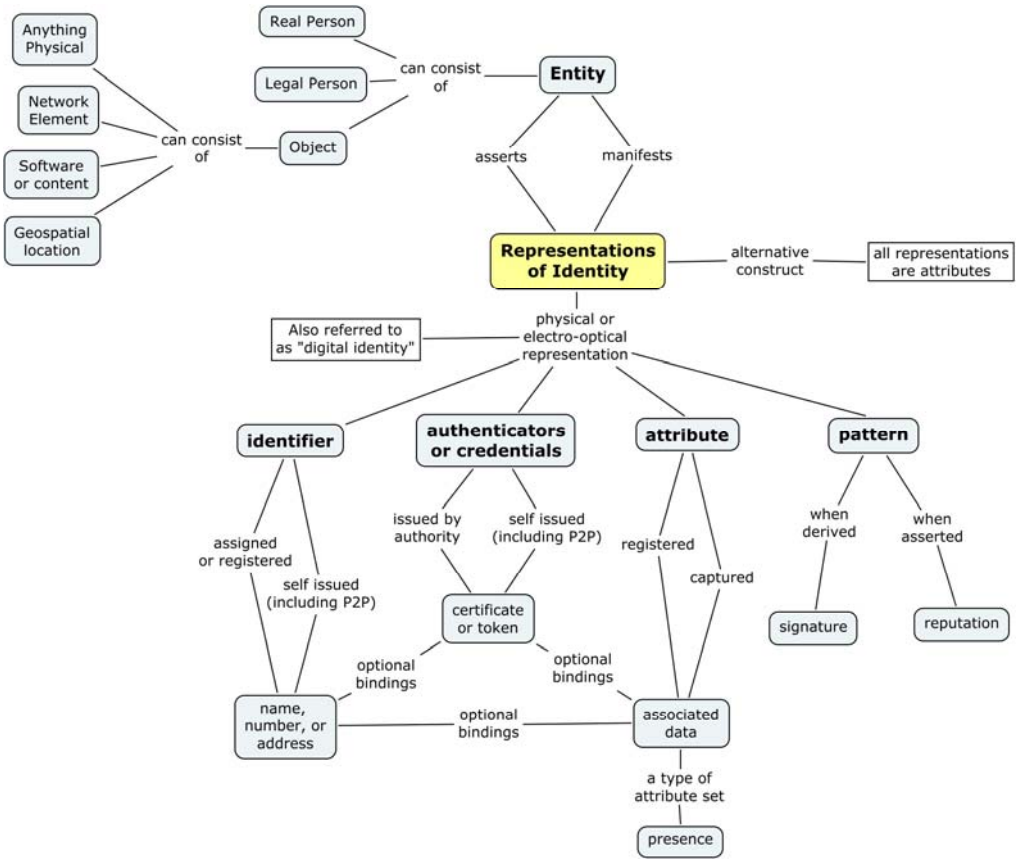
10. Ontology and Definition of "Identity" and "Identity Management

10.1 The term "identity"

Perhaps the most basic objective of the Correspondence Group is to develop a common understanding of the term "identity" that can be expressed in one or more ways to meet the needs and expectations of ITU members. Such an activity is often referred to as one of "ontology."

It seems apparent from all the uses of "identity" within past and current ITU activities and specifications, that "identity" is not anything absolute or singular or even tangible, but rather a concept that allows for various kinds of representations of an entity at some point in time and space with some degree of desired consistency. Indeed, the word "identity" is derived from the Latin word for sameness - "idem." A mandatory property of an entity from an identity perspective is sameness within some context – whether individual or collective. Identity can also be regarded as the union of all properties of an entity and things like credentials that are assigned to the entity.

Figure 1, below, attempts to organize the different aspects of identity in a common depiction. Subsequent ontology discussions make reference to this depiction.



As noted, an entity is a real person, legal person or object – which in turn can consist of anything physical, network elements, or software or content. In Open Systems Interconnection (OSI) treatment of identity, including ITU-T/ISO-IEC Object IDentifier (OID) standards today, all entities are treated only as objects. Almost every treatment of the term and concept of "identity" is with reference to these kinds of entities.

The use of "representations of identity" emerged as a good consensus term for all uses of the term "identity." The term "subject" is sometimes used within some identity community work, and at the ITU-T Seoul meeting of the IdM GSI, the term "digital subject" was discussed during the dialogue on data models as an alternative to "representations," but ultimately the latter emerged as a preferred term among the participants. In all known uses of the term "identity, it is a set of representations that are either asserted or manifested by an entity. Representations can be either "asserted" by the entity itself (effectively saying, "this is my identity") or "manifested" as representations that constitute an observed identity. Identity trust levels are typically enhanced by consistency among asserted and manifested identity representations.

Although some treatments of identity characterize all identity representations as "attributes," the more seemingly complete and comprehensive characterizations encompass four distinct kinds of representations: identifiers, authenticators or credentials, attributes, and patterns. Although these identity representations are sometimes referred to as "digital identity," in actuality they take some kind of physical or electo-optical form – some of which may consist of digital expressions. Identity is represented (especially in the ICT arena) as data in some coded form - only a subset of which is explicitly generally treated as Identity.

Identifiers (trusted or otherwise) – which are rather universally regarded as "names, numbers, or addresses" - seem to clearly constitute only one kind of identity representation. Identifiers also seem to arise in two different ways: assigned or registered by some authority, or self issued as occurs especially in peer-to-peer identity contexts.

Authenticators or credentials are certificates or tokens that some kind of revocable physical or mathematical mechanism to ensure their integrity and have bindings to an identifier or an attribute or both. Authenticators or credentials can consist of physically complex verifiable object, or a mathematical algorithm that may be paired with an associated private key, or be a password. Like identifiers, they may be issued by established authority or self issued, including those established among peers. The best know and most widely deployed and trusted electronic credentials are ITU-T X.509 digital certificates.

Attributes consist of any kind of information with a binding to an identifier or authenticator that is either registered when the identifier or authenticator is obtained, or captured in conjunction with their use. Geospatial location, transactional activity, and images are examples of the latter. One particular set of attributes is sometimes structured as "presence" – maintained entity object agent referred to as the "presentity" (a term derived from presence entity) – usually with bindings to a person.

Patterns are the last of the four kinds of identity representations, and take the form of either signatures derived from activity, or reputation when asserted by an entity for identity purposes. Examples of the former are repetitive behavior of some kind that is associated with the entity. The latter typically consist of attestations by third parties that can be associated with the entity.

In light of all of the above Sec. 10.1 analysis, if it is necessary to describe or define "identity," it is suggested that the following definition be used.

> **identity**. The assertion or manifestation of a structured representation of an entity in the form of one or more credentials, identifiers, attributes, or patterns. Such representations can take any physical or electro-optical form or syntax, and have associated implicit or explicit time-stamp and location specifications.

This definition is not constrained to any particular communication media or context, and is thus suitable for all uses within the ITU for all ICT implementations, including radio systems.

Because identifiers are one the four possible constituents of identity, the term "identifier" cannot be regarded as a replacement for "identity." It is not also apparent that the term "trusted identifier" has ever been used within the ITU or industry forums.

10.2 The term "identity management"

The term "identity management" seems universally to mean management of the representations of properties of an entity and the associated data as described in Sec. 10.2, above, and not management of "sameness or the properties of the entity itself. What is actually being managed is the entity's identity representation as data.

The use of "identity" in the essentially ubiquitous phrase "identity management," can be described or defined as follows.

> **identity management.** The diverse arrays of different technical, operational, and legal systems and practices involving the structured capture, syntactical expression, storage, tagging, retrieval, and destruction of entity identities.

11. Other Aspects of the Correspondence Group Work

During the ITU-T discussions concerning use of the term “identity,” reference was made to possible legal implications, such as a possible shifting in burdens of proof possibly associated with use of the term “identity,” or mistaken impressions regarding “absolute identity.” The Correspondence Group was unable to discover a basis for these assertions.