United Nations A/CN.9/WG.IV/WP.143

General Assembly

Distr.: Limited
10 February 2017

Original: English

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-fifth session
New York, 24-28 April 2017

Legal issues related to identity management and trust services

Terms and concepts relevant to identity management and trust services

Note by the Secretariat

Contents

V.17-00831 (E)

I. Introduction

1. At its forty-eighth session, in 2015, the Commission instructed the Secretariat to conduct preparatory work on identity management and trust services, cloud computing and mobile commerce, including through the organization of colloquia and expert group meetings, for future discussion at the Working Group level. The Commission also asked the Secretariat to share the result of that preparatory work with Working Group IV, with a view to seeking recommendations on the exact scope, possible methodology and priorities for the consideration of the Commission at its forty-ninth session.[1]

2. At its forty-ninth session, in 2016, the Commission had before it a note by the Secretariat on legal issues related to identity management and trust services (A/CN.9/891) summarizing the discussions during the UNCITRAL Colloquium on Legal Issues Related to Identity Management and Trust Services held in Vienna on 21 and 22 April 2016 and complemented by other material. The Commission was also informed that work on contractual aspects of cloud computing had started at the expert level on the basis of a proposal (A/CN.9/856) submitted at the forty-eighth session of the Commission, in 2015.[2]

3. At its fifty-fourth session (Vienna, 31 October-4 November 2016), the Working Group agreed that its future work on identity management and trust services should be limited to the use of identity management systems for commercial purposes and that it should not take into account the private or public nature of the identity management services provider. The Working Group also agreed that, while work on identity management could be taken up before work on trust services, the identification and definition of terms relevant for identity management and trust services should take place simultaneously given the close relationship between the two. It was further agreed that focus should be placed on multi-party identity systems and on natural and legal persons, without excluding consideration of two-party identity systems and of physical and digital objects when appropriate. In addition, it was agreed that the Working Group should continue its work by further clarifying the goals of the project, specifying its scope, identifying applicable general principles and drafting necessary definitions (A/CN.9/897, paras. 118-120 and 122).

4. This note contains the definition of a number of terms relevant for identity management and trust services. The terms are presented with a view to enabling discussions based on a common understanding of fundamental notions; they are not presented in order to suggest a discussion on legally binding definitions of those notions. Similarly, the terms are not intended to provide an indication on the scope of the future work of UNCITRAL in the field of identity management and trust services.

5. The source of the defined terms, where available, is explicity indicated. Due to different sources, the same term may include more than one definition. If no source is indicated, the definition was suggested during expert consultations. Preference was given to terms defined internationally. Additional sources of defined terms are available, especially at the national level.

6. The defined terms are listed in different sections for ease of presentation only and without prejudice to the determinations of the Working Group on their relevance for discussions on the legal aspects of identity management or of trust services.

---

[1] *Official Records of the General Assembly*, *Seventieth Session, Supplement No. 17* (A/70/17), para. 358.

[2] Ibid., *Seventy-first Session, Supplement No. 17* (A/71/17), para. 229.

7. The defined terms have different origins and therefore should not be read as a coherent set of interconnected terms. Rather, each term should be read separately as a stand-alone definition and as such is presented as a possible reference for the discussions of the Working Group. When available, the source of the defined term is indicated so that additional information could be gathered from the original source document.

8. Synonyms are indicated for convenience only in light of usage. Not all synonyms are terms defined in this note.

9. The terms are listed in alphabetical order in the English language version of this note. The same order is maintained in other language versions to ensure correspondence of paragraphs and therefore facilitate reference during the Working Group discussions.

II. Terms and concepts relevant to identity management and trust services

A. Definitions relevant to identity management

10. "Assurance level" means a level of confidence in the binding between an entity and the presented identity information. Source: Rec. ITU-T X.1252. Synonyms: identity assurance, level of assurance.

11. "Attribute" means an item of information or data associated with a subject. Examples of attributes include information such as name, address, age, gender, title, salary, net worth, driver's license number, social security number, e-mail address, mobile number, and data such as the subject's network presence, the device used by the subject, the subject's usual home location as known by a network, etc. (for a human being); corporate name, principal office address, registration name, jurisdiction of registration, etc. (for a legal entity); make and model, serial number, location, capacity, device type, etc. (for a device). Synonym: identity attribute.

12. "Attribute provider" means a business or government entity that acts as a source of one or more attributes of a subject's identity. An attribute provider is often the entity responsible for assigning, collecting, or maintaining such attributes. Examples of attribute providers include a government agency that maintains a birth registry or title registry, a national credit bureau, a business that maintains a commercial marketing database or a corporate registry, and entities such as mobile operators, banks, utilities and healthcare providers that hold verified user data and that either verify or provide these attributes to third parties (possibly, subject to user consent).

13. "Authentication" means (a) a process used to achieve sufficient confidence in the binding between the entity and the presented identity. Source: Rec. ITU-T X.1252; (b) the process of associating the claimed identity of a subject with the actual subject by confirming the subject's association with a credential either directly (active authentication) or through the environment in which the subject is interacting ("passive authentication" or "adaptive authentication"). For example, entering a secret password that is associated with a username is assumed to authenticate that the individual entering the secret password is the person to whom the username was issued. Likewise, comparing a person presenting a passport to the picture appearing on the passport is used to authenticate (i.e., confirm) that that person is the person described in the passport.

14. "Authentication assurance" means 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. Source: Rec. ITU-T X.1252. Note: in some cases, the notions of "identity assurance" and "authentication assurance" are viewed as separate components of the overall concept of "level of assurance".

15. "Authentication factor" means a piece of information and process used to authenticate or verify the identity of an entity. Source: ISO/IEC 19790. Note: authentication factors are divided into four categories: (a) something an entity has (e.g., device signature, passport, hardware device containing a credential, private key); (b) something an entity knows (e.g., password, PIN); (c) something an entity is (e.g., biometric characteristic); or (d) something an entity typically does (e.g., behaviour pattern). Source: Rec. ITU-T X.1254.

16. "Authenticator" means something that is used to verify the relationship between a subject and a credential. An active authenticator is usually something the subject knows (such as a secret password), something the subject has (such as a smartcard), or something the subject is (such as a photo or other biometric information), and is used to tie the subject to an identity credential. For example, a password functions as an authenticator for a username, a picture functions as an authenticator for a passport or driver's license. A passive authenticator is usually something the environment knows, e.g. the mobile network knows that the user is connected to the network, is in the usual location, is using the usual mobile device, has not been barred from using the network, etc.

17. "Authoritative source" means a repository which is recognized as being an accurate and up-to-date source of information. Source: Rec. ITU-T X.1254.

18. "Authorization" means (a) a process of granting rights and privileges to an authenticated subject based on criteria usually determined by the relying party. For example, once a subject is authenticated, he or she might be granted access to a confidential database. Source: A/CN.9/WG.IV/WP.120, annex; (b) the granting of rights and, based on these rights, the granting of access. Source: Rec. ITU-T Y.2720 and Rec. ITU-T X.800.

19. "Credential" means: (a) a set of data presented as evidence of a claimed identity and/or entitlements. Source: Rec. ITU-T X.1252; (b) data in digital or tangible form presented as evidence of a claimed identity of a subject. Examples of paper-based credentials include passports, birth certificates, driver's licenses, and employee identity cards. Examples of digital credentials include usernames, smart cards, mobile identity and digital certificates. Source: A/CN.9/WG.IV/WP.120, annex. Synonyms: electronic identification means, identity credential.

20. "Credential provider" or "Credential service provider" means (a) an entity that issues credentials to subjects; (b) a trusted actor that issues and/or manages credentials. Note: the Credential Service Provider (CSP) may encompass Registration Authorities (RAs) and verifiers that it operates. A CSP may be an independent third party, or it may issue credentials for its own use. Source: Rec. ITU-T X.1254.

21. "Enrolment" means (a) 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. Source: Rec. ITU-T X.1252; (b) the process by which credential providers (or their agents) verify the identity claims of a subject before issuing a credential to such subject.

22. "Entity" means something that has separate and distinct existence and that can be identified in a 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. Source: Rec. ITU-T X.1252. An entity may have multiple identifiers.

23. "Federation" means (a) an association of users, service providers, and identity service providers. Source: Rec. ITU-T X.1252; (b) a group of identity providers, relying parties, subjects and others that agree to operate under compatible policies, standards, and technologies specified in system rules (or a trust framework) in order that subject identity information provided by identity providers can be understood and trusted by relying parties. Synonyms: identity federation, multi-party identity system.

24. "Identification" means the process of collecting, verifying, and validating sufficient identity attributes about a specific subject to define and confirm its identity within a specific context. Synonyms: identity proofing, registration.

25. "Identifier" means (a) one or more attributes used to identify an entity within a context. Source: Rec. ITU-T X.1252; (b) one or more attributes that uniquely characterize an entity in a specific context. Source: Rec. ITU-T X.1254.

26. "Identity" means (a) a set of attributes related to an entity. Source: ISO/IEC 24760; (b) information about a specific subject in the form of one or more attributes that allow the subject to be sufficiently distinguished within a particular context; (c) a set of the attributes about a person that uniquely describes the person within a given context. Synonym: digital identity.

27. "Identity assertion" means an electronic record originating with an identity provider and sent to a relying party that contains the subject's identifier (e.g., name, account number, mobile number, location, etc.), authentication status, and applicable identity attributes. The attributes are typically personal and non-personal information about the subject that is relevant to the transaction required by the relying party.

28. "Identity assurance" means 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. Source: Rec. ITU-T X.1252. Synonyms: assurance level; level of assurance. Note: in some cases, the notions of "identity assurance" and "authentication assurance" are viewed as separate components of the overall concept of "level of assurance".

29. "Identity federation" means a group of identity providers, relying parties, subjects and others that agree to operate under compatible policies, standards, and technologies specified in system rules (or a trust framework) in order that subject identity information provided by identity providers can be understood and trusted by relying parties. See also: federation; multi-party identity system.

30. "Identity management" means (a) a set of processes to manage the identification, authentication, and authorization of individuals, legal entities, devices, or other subjects in an online context. Source: A/CN.9/854, paragraph 6; (b) 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: (i) assurance of identity information (e.g., identifiers, credentials, attributes); (ii) assurance of the identity of an entity; and (iii) enabling business and security applications. Source: Rec. ITU-T Y.2720.

31. "Identity proofing" means (a) the process of collecting, verifying, and validating sufficient identity attribute information about a specific subject (a person, legal entity, device, digital object, or other entity) to define and confirm its identity within a

specific context. Identity proofing may be carried out through self-assertion or against existing records; (b) a process which validates and verifies sufficient information to confirm the claimed identity of the entity. Source: Rec. ITU-T X.1252; (c) a process by which a registration authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance. Source: Rec. ITU-T X.1254. Synonyms: identification; registration.

32. "Identity provider" means (a) an entity responsible for the identification of persons, legal entities, devices, and/or digital objects, the issuance of corresponding identity credentials, and the maintenance and management of such identity information for subjects. Source: A/CN.9/WG.IV/WP.120, annex; (b) an entity that creates, maintains and manages trusted identity information of other entities (e.g., users/subscribers, organizations and devices) and offers identity-based services based on trust, business and other types of relationship. Source: Rec. ITU-T Y.2720. Synonym: credential service provider; identity service provider.

33. "Identity system" means an online environment for identity management transactions governed by a set of system rules (also referred to as a trust framework) where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their identities. Source: A/CN.9/WG.IV/WP.120, annex. An identity system involves (a) a set of rules, methods, procedures and routines, technology, standards, policies, and processes, (b) applicable to a group of participating entities, (c) governing the collection, verification, storage, exchange, authentication, and reliance on identity attribute information about an individual person, a legal entity, device, or digital object, (d) for the purpose of facilitating identity transactions. Synonyms: identity management system ("IdM system"); identity federation; electronic identification scheme.

34. "Identity transaction" means any transaction involving two or more participants which involves establishing, verifying, issuing, asserting, revoking, communicating, or relying on identity information.

35. "Identity verification" means the process of confirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information. Source: Rec. ITU-T X.1252.

36. "Level of assurance" means a designation of the degree of confidence in the identification and authentication processes — i.e., (a) the degree of confidence in the vetting process used to establish the identity of an entity to whom a credential was issued, and (b) the degree of confidence that the entity using the credential is the entity to whom the credential was issued. The assurance reflects the reliability of methods, processes and technologies used. Some level of assurance schemes define levels of assurance by number, i.e., Levels 1 to 4, where Level 1 is the lowest assurance level, and Level 4 is the highest. Other schemes designate assurance levels as "low," "substantial" and "high". Synonyms: assurance level; identity assurance; trust level.

37. "Multifactor authentication" means authentication with at least two independent authentication factors. Note: authentication factors are divided into four categories: (a) something an entity has (e.g., device signature, passport, hardware device containing a credential, private key); (b) something an entity knows (e.g., password, PIN); (c) something an entity is (e.g., biometric characteristic); or (d) something an entity typically does (e.g., behaviour pattern). Source: ISO/IEC 19790; Rec. ITU-T X.1254

38. "Multi-party identity system" means an identity system, also referred to as an identity federation, in which a subject can use an identity credential issued by any one of several identity providers to authenticate multiple unrelated relying parties; An identity system that allows the use of identity credentials issued, and identity

information asserted, by one or more identity providers with multiple relying parties. Source: A/CN.9/WG.IV/WP.120, annex. Synonym: identity federation.

39. “Participant” means any person or legal entity that participates in an identity system or an identity transaction using such system. Participants include subjects, identity providers, attribute providers, credential providers, relying parties, identity system operators, and others. Like participants in a credit card system, participants in an identity system typically agree contractually to a set of system rules (often referred to as a trust framework) applicable to their role.

40. “Proofing” means the verification and validation of information when enrolling new entities into identity systems. Source: Rec. ITU-T X.1252. Synonyms: identity proofing, identification.

41. “Pseudonym” means 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. Source: Rec. ITU-T X.1252.

42. “Registration” means 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. Source: Rec. ITU-T X.1252.

43. “Registration authority” means an entity that provides enrolment and/or identity proofing services in the context of a federated (i.e., multi-party) identity system, usually for an identity provider.

44. “Relying party” means (a) the person or legal entity that relies on an identity credential or identity assertion to make a decision as to what action to take in a given application context, such as to process a transaction or grant access to information or a system. Source: A/CN.9/WG.IV/WP.120, annex; (b) an entity that relies on an identity representation or claim by a requesting/asserting entity within some request context. Source: Rec. ITU-T X.1252; (c) a natural or legal person that relies upon an electronic identification or a trust service. Source: Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (“eIDAS”), article 3(6).

45. “Repository” means an interface that accepts deposits of digital entities, enables their retention, and provides secure access to the digital entities via their identifiers. Source: Rec. ITU-T X.1255.

46. “Role” means a type (or category) of participant in an identity system, such as a subject, identity provider, credential provider, relying party, etc. A participant may have multiple roles. For example, with respect to the identification of its employees, an employer may function as both an identity provider and a relying party.

47. “Self-asserted identity” means an identity that an entity declares to be its own. Source: Rec. ITU-T X.1252.

48. “Subject” means the person, legal entity, device, or digital object (i.e., the entity) that is identified in a particular identity credential and that can be authenticated and vouched for by an identity provider. Source: A/CN.9/WG.IV/WP.120, annex. Synonyms: user; data subject.

49. “System rules”: see trust framework.

50. “Trust” means 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. Source: Rec. ITU-T X.1252.

51. “Trust framework” means (a) the system rules for an identity system consisting of the business, technical, and legal rules that govern the participation in and operation of a specific identity system. They are typically privately developed (e.g., by the identity system operator of a specific identity system), and made binding and enforceable on the participants via contract. Source: A/CN.9/WG.IV/WP.120, annex; (b) a set of requirements and enforcement mechanisms for parties exchanging identity information. Source: Rec. ITU-T X.1254; (c) an IdM system where a set of verifiable commitments made by each of the various parties in a transaction to their counter parties, and these commitments necessarily include: (i) controls to help ensure commitments are met and (ii) remedies for failure to meet such commitments. Source: Rec. ITU-T X.1255. Synonyms: system rules; operating rules; scheme rules.

52. “Trust framework provider” means the entity or organization that creates or adopts the system rules and associated contractual structure for a specific identity system. The trust framework provider may also certify the participants that are in compliance with those system rules. For example, credit and debit card issuers may fulfill a similar role in the credit and debit card world; they set forth the system rules and enforce compliance.

53. “Trusted third party” means (a) an authority or its agent, trusted by other actors with respect to other activities (e.g., security related activities). Source: Rec. ITU-T X.1254; (b) an entity accepted by all parties to a transaction as an impartial and trustworthy intermediary to facilitate interactions between and among the parties.

54. “User” means (a) a subject of a credential; a consumer of the services offered by a relying party; (b) any entity that makes use of a resource, e.g., system, equipment, terminal, process, application, or corporate network. Source: Rec. ITU-T X.1252.

55. “Validation” means the process of verifying and confirming that an identity credential is valid (e.g., that it has not expired or been revoked).

56. “Verification” means (a) the process of checking information by comparing the provided information with previously corroborated information. Source: Rec. ITU-T X.1254; (b) 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. Source: Rec. ITU-T X.1252.

B. Definitions relevant to trust services

57. The following definitions may be particularly relevant in discussions on the legal aspects of trust services. However, a number of the definitions listed as relevant to the discussions on legal aspects of identity management may also be relevant for the discussions on the legal aspects of trust services (see above, para. 6).

58. “Certification service provider” means a person that issues certificates and may provide other services related to electronic signatures; Source: UNCITRAL Model Law on Electronic Signatures, article 2(e).[3]

59. “Electronic registered delivery service” means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the

[3] United Nations publication, Sales No. E.02.V.8.

data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations. Source: eIDAS, article 3(36).

60. "Electronic seal" means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity. Source: eIDAS, article 3(25).

61. "Electronic signature" means (a) data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Source: eIDAS, article 3(10); (b) data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message. Source: UNCITRAL Model Law on Electronic Signatures, article 2(a). Note: article 9(3)(a) of the United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)[4] refers to indication of the signatory's intention in respect of the information contained in the electronic communication.

62. "Electronic time stamp" means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time. Source: eIDAS, article 3(33).

63. "Relying party" means a person that may act on the basis of a certificate or an electronic signature. Source: UNCITRAL Model Law on Electronic Signatures, article 2(f).

64. "Trust service" means an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services. Source: eIDAS, article 3(16).

65. "Trust service provider" means a natural or a legal person who provides one or more trust services [either as a qualified or as a non-qualified trust service provider]. Source: eIDAS, article 3(19).

66. "Time stamp" means a reliable time variant parameter which denotes a point in time with respect to a common reference. Source: Rec. ITU-T X.1254.

67. "Validation" means the process of verifying and confirming that an electronic signature or a seal is valid. Source: eIDAS, article 3(41).

[4] General Assembly resolution 60/21, annex.