International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1252

(04/2021)

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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 defines 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. Recommendation ITU-T X.1252 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. Recommendation ITU-T X.1252 includes an annex that explains the rationale for some of these key terms.

One of the main objectives of Recommendation ITU-T X.1252 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	Unique ID*
1.0	ITU-T X.1252	2010-04-16	17	11.1002/1000/10440
2.0	ITU-T X.1252	2021-04-30	17	11.1002/1000/14642

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Page

Recommendation ITU-T X.1252

Baseline identity management terms and definitions

1 Scope

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

None.

3 Definitions

Compiled IdM terms and definitions are listed in clause 6.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CID	Cryptographic Identifier
DDO	DID Object Descriptor
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
ID	Identifier
IdM	Identity Management
IdP	Identity Provider
IdSP	Identity Service Provider
IH	Identity Hub
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RA	Registration Authority
RE	Requesting Entity
RP	Relying Party
SIM	Subscriber Identity Module

SSI	Self-Sovereign Identity
URL	Uniform Resource Locator
ZKP	Zero-Knowledge Proof

5 Conventions

None.

6 Terms and definitions

6.1 **access control**: A procedure by which an administrator can restrict 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**: Identifies a specific network termination point and can be used for routing to this physical and logical termination point inside a public or private network.

NOTE – Based on [b-ITU-T E.101].

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

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

6.5 **anonym**: An identifier used exactly once.

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

NOTE – Anonymity can prevent the tracking, tracing, and fingerprinting of entities or their behaviour, such as user location and usage frequency of a service.

6.7 **assertion**: A statement made by an entity without accompanying evidence of its validity.

NOTE – The terms assertion and claim [*noun*] are agreed to be very similar.

6.8 **assurance**

NOTE –See authentication assurance and identity assurance.

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

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

6.11 **attribute type** [b-ITU-T X.501]: That component of an attribute which indicates the class of information given by that attribute.

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

6.13 **authentication** [b-ISO/IEC 24760-1]: Formalized process of verification that, if successful, results in an authenticated identity for an entity.

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

6.14 **authentication assurance**: Positive acknowledgement in the authentication process intended to provide confidence that the communication partner is the entity that it claims to be or is expected to be.

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

6.15 **authorization**: The granting of rights and, based on these rights, the granting of access.

NOTE – Based on [b-ITU-T X.800].

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

6.17 biometric recognition; biometrics [b-ISO/IEC 2382-37]: Automated recognition of individuals based on their biological and behavioural characteristics.

6.18 certificate: 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.

NOTE – Based on a definition of "security certificate" in [b-ITU-T X.810].

6.19 claim: [*noun*] Digital assertion about identity attributes made by an entity about itself or another entity. [*verb*] To state as being the case, without being able to give proof.

NOTE – The terms assertion and claim [*noun*] are agreed to be very similar.

6.20 claimant: An entity that is or represents a principal for the purposes of authentication.

NOTE 1 – A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

NOTE 2 – Based on [b-ITU-T X.811].

6.21 claim definition: A machine-readable definition of the semantic structure of a claim.

NOTE – Claim definitions facilitate interoperability of claims and proofs across multiple issuers, holders, and relying parties.

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

6.23 correlation: The combination of various pieces of information that are related to an entity or become related to an entity when combined.

NOTE – Correlation is closely associated with identification. Correlation can facilitate identification and the inference of information about an entity that is not directly provided by the data given.

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

NOTE – [b-ISO/IEC 29115] is a similar text to [b-ITU-T X.1254] and contains the same definition of credential that was developed by the groups involved.

6.25 data minimization: Limiting collection, storage, and use of identifiers, attributes and other data associated with an entity to only what is necessary to perform authentication, and limiting any exchange and disclosure of data associated with an entity, including contextual information of a request, to only what is necessary for responding to the request and to only the relying party associated with the request.

6.26 decentralized identifier (DID): A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network. A DID is associated with exactly one DID object descriptor.

NOTE – See [b-W3C-DIDs].

6.27 DID object descriptor (DDO): A set of data describing the decentralized identifier (DID) subject, including mechanisms, such as cryptographic public keys, that the DID subject or a DID delegate can use to authenticate itself and prove its association with the DID.

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

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

6.30 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

6.31 decentralized key management system: A standard for interoperable cryptographic key management based on decentralized identifiers.

6.32 domain: An environment in which an entity can use a set of attributes for identification and other purposes.

NOTE – A domain provides context.

6.33 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 for registration. In many cases, the latter is used to describe both processes.

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

NOTE 1 – An entity can have a physical or logical embodiment.

NOTE 2 – 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, and interfaces.

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

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

6.36 federation [b-ITU-T Y.2720]: Establishing a relationship between two or more entities or an association comprising any number of service providers and identity providers.

6.37 holder: An entity that has been issued a claim by an issuer. If the claim supports zero-knowledge proof s, the holder is also the prover.

6.38 identification [b-ISO/IEC 24760-1]: Process of recognizing an entity in a particular domain as distinct from other entities.

6.39 identifier (ID) [b-ITU-T E.101]: A series of digits, characters and symbols used to identify uniquely a subscriber, a user, a network element, a function, a network entity, a service or an application. Identifiers can be used for registration or authorization. They can be either public to all networks or private to a specific network (private IDs are normally not disclosed to third parties).

NOTE – An identifier can be a specifically created attribute with a value assigned to be unique within the domain.

6.40 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 a context. For identity management 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.

6.41 identity assurance: The confidence provided 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.

6.42 identity-based security policy [b-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.

6.43 identity management (IdM): 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 support of business and security applications.

NOTE – Based on [b-ITU-T Y.2720].

6.44 identity owner: An entity who can be held responsible. An identity owner must be either an individual or an organization. Mutually exclusive from thing.

6.45 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.

6.46 identity proofing [b-ISO/IEC 29115]: Process by which the registration authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance.

6.47 identity provider (IdP)

NOTE – See identity service provider (IdSP).

6.48 identity service bridge provider: An identity service provider (IdSP) that acts as a trusted intermediary among other IdSPs.

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

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

6.51 independent: An individual who directly controls the private key(s) and master secret(s) necessary to administer a decentralized identity.

6.52 individual: An identity owner who is a natural person. Mutually exclusive from organization.

6.53 issuer: The entity that issues a claim.

6.54 issuer key: The special type of cryptographic key necessary for an issuer to issue a claim that supports zero-knowledge proofs.

6.55 key-chain: The task of securing the storage of private keys or data on a trusted hardware unit in a device.

6.56 legal identity: A set of information sufficient to identify an identity owner for the purpose of legal accountability in at least one jurisdiction. For the purposes of a provisional network, a legal identity may be established by reference to one or more publicly accessible web resources, such as websites, blogs, social network profiles or other web pages that provide sufficient information to meet this test.

6.57 linkability: The ability to distinguish, within a set of information, whether two or more attributes, identifiers, identities or other data are related with a high enough degree of probability to be useful.

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

NOTE – Compare with assertion.

6.59 mutual authentication [b-ISO/IEC 29115]: Authentication of identities of entities which provides both entities with assurance of each other's identity.

6.60 name: A combination of characters used to identify entities (e.g., subscriber, network element) that may be resolved or translated into an address. Characters may include numbers, letters and symbols.

NOTE 1 – 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.

NOTE 2 – Based on [b-ITU-T E.101].

6.61 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.

6.62 pattern

NOTE – See identity pattern.

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

6.64 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.

6.65 principal: An entity whose identity can be authenticated.

NOTE – This entry appears in [b-ITU-T X.811], [b-ITU-T Y.2702] and [b-ITU-T Y.2720]

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

6.67 private key [b-ITU-T X.509]: (In a public-key cryptosystem) that key of an entity's key pair which is known only by that entity.

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

6.69 proof: Cryptographic verification of a claim. A digital signature is a simple form of proof. A cryptographic hash is also a form of proof. Proofs are one of two types: transparent or zero knowledge. Transparent proofs reveal all the information in a claim. Zero-knowledge proof s enable selective disclosure of the information in a claim.

6.70 prover: Entity that issues a proof from a claim. The prover is also the holder of the claim.

6.71 pseudonym [b-ISO/IEC 24760-1]: Identifier that contains the minimal identity information sufficient to allow a verifier to establish it as a link to a known identity.

NOTE 1 – A pseudonym can be an identifier with a value chosen by the person or assigned randomly.

NOTE 2 – A pseudonym can be used to avoid or reduce privacy and security risks associated with the use of identifier bindings, which may reveal the identity of the entity.

6.72 public data [b-ITU-T L.1410]: Data which is available to the public without access being restricted by requirements on membership, non-disclosure agreements, or similar restrictions.

6.73 public key [b-ITU-T X.509]: That key of an entity's key pair which is publicly known.

6.74 public profile: Information describing a service provider, including its legal identity, logo(s) or other trademarks, location(s), marketing information, web links and any other information required by the trust framework to ensure full transparency about the provider's legal identity and qualifications.

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

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

6.76 relying party (RP): An entity that relies on an identity representation or claim by a requesting or asserting entity within some request context.

NOTE – Based on [b-ITU-T Y.2720].

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

6.78 requesting entity (RE): An entity making an identity representation or claim to a relying party within some request context.

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

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

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

6.81 security audit [b-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.

6.82 security domain: 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.

NOTE – Based on [b-ITU-T X.810]. Similar definitions appear in [b-ITU-T Y.2701] and [b-ITU-T Y.2720].

6.83 security zone: A protected area characterized by operational control, location, and connectivity to other devices or network elements.

NOTE – Based on [b-ITU-T Y.2701].

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

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

6.86 thing: An entity that cannot be held legally accountable. A thing may be an animal (e.g., pet, livestock), a natural object (e.g., house, car, phone), or a digital object (e.g., software program, network service, data structure). Mutually exclusive from identity owner.

6.87 trust: The confidence of one party or entity that another party or entity will behave in a well-defined way that does not violate agreed-upon rules, policies or legal clauses of the identity management system.

6.88 trust anchor: An identity owner who may serve as a starting point in the decentralized web of trust. A trust anchor has two unique privileges:

- to add new identity owners to the network; and
- to issue trust anchor invitations.

A trust anchor must meet the trust anchor qualifications and agree to the trust anchor obligations defined in the trust framework. All trustees and stewards are automatically trust anchors.

6.89 trust framework: A legally enforceable set of specifications, rules, and agreements that governs an identity system.

NOTE – Based on [b-OIX-TFIS].

6.90 trusted third party: In the context of a security policy, a security authority or its agent that is trusted with respect to some security relevant-activities.

NOTE 1 – Based on [b-ITU-T X.810] and [b-ITU-T Y.2702].

NOTE 2 – See [b-ITU-T X.800].

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

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

6.93 **user-centric**: An identity management system that provides the user with the ability to control and enforce various policies governing user data, including personally identifiable information.

6.94 **validator node**: A node that validates new transactions of identity records and actively writes valid transactions to the ledger using the ledger consensus protocol.

6.95 **verifiable claim**: A claim that includes a proof from the issuer. Typically this proof is in the form of a digital signature. A verifiable claim may be verified by a public key associated with the issuer's decentralized identifier.

NOTE – Based on [b-W3C-VC].

6.96 **verification** [b-ISO/IEC 24760-1]: Process of establishing that identity information associated with a particular entity is correct.

NOTE 1 – The process of identification applies verification to claimed or observed attributes.

NOTE 2 – Verification of (identity) information may encompass examination with respect to validity, correct source, original, (unaltered), correctness, binding to the entity, etc.

NOTE 3 – Information is correct at the time of verification.

6.97 **verifier** [b-ISO/IEC 24760-1]: Entity that performs verification.

6.98 **wallet (identity wallet)**: An application that primarily allows a user to hold identifiers and credentials by storing the corresponding private keys on the user device.

6.99 **zero knowledge proof (ZKP)**: A proof that uses special cryptography and a master secret to permit selective disclosure of information in a set of claims. A ZKP proves that some or all of the data in a set of claims is true without revealing any additional information, including the identity of the prover.

NOTE 1 – The notion of "selective disclosure" means a wide range of choice for disclosure. For example, ZKPs can be used to prove numerous claims about confidential data such as: (1) adulthood, without revealing the birth date; (2) solvency (not being bankrupt), without showing the portfolio composition; (3) ownership of an asset, without revealing or linking to past transactions.

NOTE 2 – Based on [b-ITU-T X.1403].

Annex A

Key points and rationale for identity management basic terminology

(This annex forms an integral part of this Recommendation.)

Background

Discussions on IdM have illustrated differences in understanding that people have about its intention, the basic procedures used and the 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 records 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 IdM.

Introduction

Identity is the term around which all other IdM terms revolve. In the real rather than the 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 and behaviour. Others, like date of birth, place of birth, home address and telephone number, may also be used. In a communication process, both parties normally require sufficient confidence that they are communicating with the correct partner. This process of seeking confidence often involves two or more individuals or "entities": the entity whose identity is to be confirmed – the requesting entity (RE), and the entity that will rely on a confirmed identity – the RP. A third entity that manages identities may be involved – an IdSP.

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 (IDs) 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. This clause helps to explain the authentication process and its relevance to confidence.

Note that, when applying this model to real procedures and applications, clarity about the relevant communication partners and the applicable chains of trust is required.

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 1 – An entity can have a physical or logical embodiment.

NOTE 2 – 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, and interfaces.

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 in a particular domain as distinct from other entities.

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 may also 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.

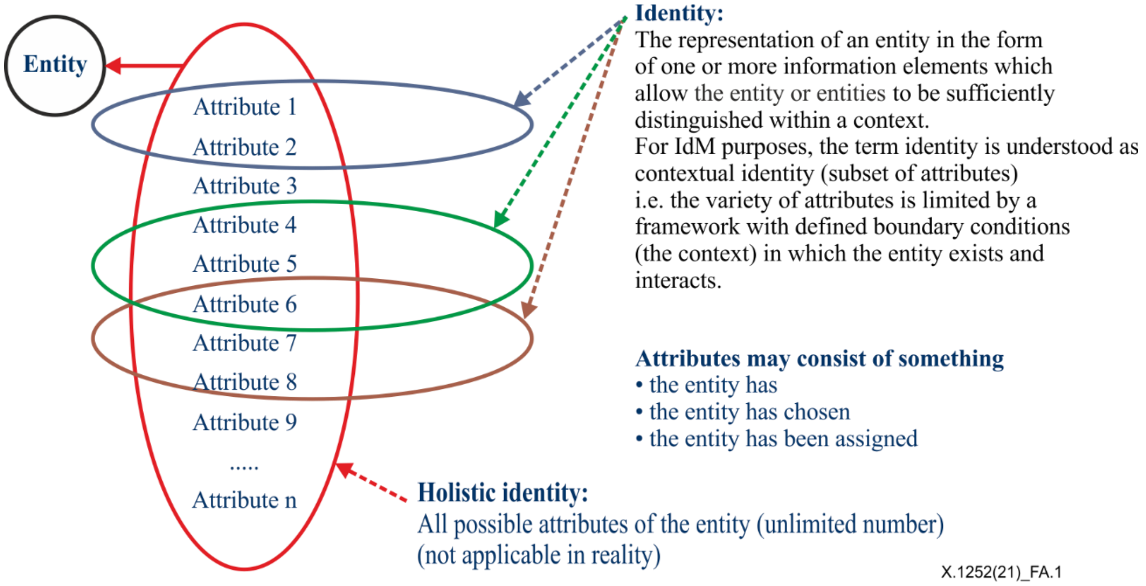

Entity
Attribute 1
Attribute 2
Attribute 3
Attribute 4
Attribute 5
Attribute 6
Attribute 7
Attribute 8
Attribute 9
.....
Attribute n
Identity:
The representation of an entity in the form of one or more information elements which allow the entity or entities to be sufficiently distinguished within a context.
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(21)_FA.1

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

As already noted, authentication is relevant for IdM. 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 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:

- sharing or delivery of information that is not intended to be available to everybody;
- granting access to:
  - information,
  - rooms, areas or domains,
  - services
  - usage of resources;
- making contracts.

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

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 RE, entity X acts as RP.

Authentication of X: Entity X acts as RE, Y acts as RP.

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 RP,
- sufficient trust that the RP 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 username and password).

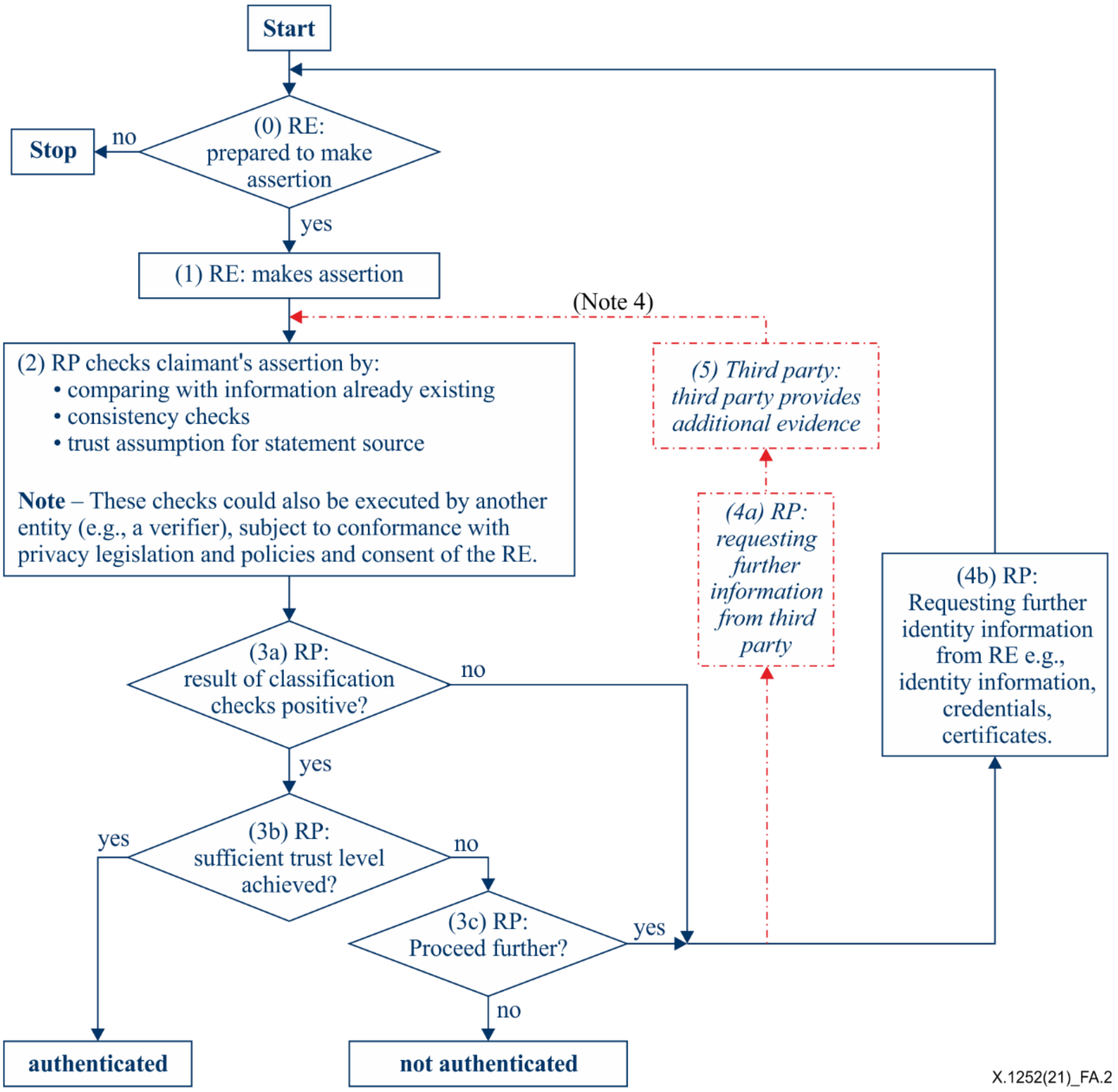
In some cases (but not in user-centric systems), a third party could be directly involved to provide further information as evidence to the RP to improve trust in the attributes of the RE.

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);
- at which the entity is located;
- combination of these.

Identities can be checked by:

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


Start
(0) RE: prepared to make assertion
no
Stop
yes
(1) RE: makes assertion
(Note 4)
(2) RP checks claimant's assertion by:
• comparing with information already existing
• consistency checks
• trust assumption for statement source
Note – These checks could also be executed by another entity (e.g., a verifier), subject to conformance with privacy legislation and policies and consent of the RE.
(5) Third party: third party provides additional evidence
(4a) RP: requesting further information from third party
(4b) RP: Requesting further identity information from RE e.g., identity information, credentials, certificates.
(3a) RP: result of classification checks positive?
no
yes
(3b) RP: sufficient trust level achieved?
yes
no
(3c) RP: Proceed further?
yes
no
authenticated
not authenticated
X.1252(21)_FA.2

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

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 flowchart example in Figure A.2, it is always up to the RP to decide whether to accept the RE 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 IdM, 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 have 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 subscriber identity module (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.

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 or assertion

The meanings of the terms claim and assertion are generally agreed to be somewhat similar, but with slightly different significance. In some cases, an assertion is considered to be a stronger statement than a claim. For example, claim can be defined 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 adjectives "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 whatsoever. It will always be up to the RP to decide whether to accept the claim or assertion based on verification by the RP (or by a verifier acting at the request of the RP).

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 for 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 (IdP) and IdSP are both commonly used. Although the term IdP 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 them. 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 and financial service provider.

The term IdSP is, therefore, seen as somewhat more descriptive than IdP 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 IdP for IdSP and retaining the term IdP but, instead of defining it, simply providing a pointer to 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 that is observed or recognized and for which a structure can be detected or that fits into an already known structure.

For example, two 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 one. Also, an identity pattern can be based on more than an activity or behaviour and is not limited to information that 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 situations could also be conceived in which 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 ones.

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 a 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 involving consumption of certain medicines.

Annex B

Key points and rationale for decentralized identity management basic terminology

(This annex forms an integral part of this Recommendation.)

B.1 Decentralized identity

Identity models as presented in Annex A are IdP-centric. The model assumes that users rely on IdPs for establishing, mainlining and providing them with identities to use for their online interactions. This IdP-centric approach for identity requires users to trust IdPs with their identities. In the IdP-centric approach, federation services are offered by the IdPs for identity re-use. The ability to reuse a user identity is limited by federation members. Identity federation puts providers at the centre of trust, with their focus on protecting their business model as opposed to the enablement of a true decentralized identity echo system that allows users to be in charge of their identity and relationships. The IdP-centric identity model requires implicit trust in centralized IdPs. As such the model is not flexible and not dynamic.

On the other hand, in the decentralized identity model, the system enables users to be in control of their own identity. In the decentralized approach, providers focus on asserting claims about specific identities. Decentralized identity models are fuelled by the current development of distributed ledger technologies (DLTs).

In order to enable services across participating domains, centralized identity models focus on providing authentication services in one domain to enable access through identity federation bridges to another. In online interactions, the pressure is on identity-based systems to confirm the claimed identity of the entity as opposed to provide access control. As such, a major function of decentralized identity systems is to provide a model to enable the delivery of assertions about the identity of a user that can be easily used across providers.

A user-centric identity model consists of individual or administrative control across multiple identity domains without the need of a federation acting as a trust circle. User-centric identity aims to create a persistent online identity for an entity that is focused on creating a better online experience while providing users better control over their identities through the use of decentralized trust models. However, due to the lack of simplicity and lack of technologies such as DLTs, the user-centric model did not succeed.

The concept of a user-centric identity is gaining traction since the introduction of DLTs. A protocol stack is being developed that builds on DLT to enable a true decentralized identity infrastructure. These systems can be powered by public, private, permissionless or permissioned DLTs to enable the management of digital identities. The goal is to transition the control of identity assertions back to users while maintaining system security, integrity and privacy.

B.2 Decentralized identity model

Decentralized identity is a model that promotes individual control (with ability to delegate control) across any number of authorities (including IdPs). One specific model of decentralized identity is called self-sovereign identity (SSI) which has the assumptions listed in Table B.1.

Table B.1 – Self-sovereign identity assumptions

Existence	Users must have an independent existence
Control	Users must control their identities
Access	Users must have access to their own data
Transparency	Systems and algorithms must be transparent
Persistence	Identities must be long-lived
Portability	Information and services about identity must be transportable
Interoperability	Identities should be as widely usable as possible
Consent	Users must agree to the use of their identity
Minimization	Disclosure of claims must be minimized
Protection	The rights of users must be protected

The desired aspects are very much in line with what DLT can offer. Decentralized identity implementations are usually based around claims and attestations in which actors can often play different roles.

Decentralized identity systems can be used to facilitate trusted online transactions. Decentralized identity systems enable users to prove attributes about themselves to a services provider (or *vice versa*) through the use of verifiable claims (attestations). The whole process can be done in an interoperable and trusted fashion through the use of a technological stack that enables the dissemination of trusted claims without the need for direct relationships between transaction participants.

In a decentralized identity system, the service provider is acting as an RP, while claims are provided by an attestation issuer, who issues missing attestations that are required. An attestation is a collection of statements about the accuracy of another collection of statements. The original set of statements can also be named a claim. The receiver of an attestation should be able to validate the commitment of the attester to the claims. The commitment should thus be in the form of a digital signature or a pointer to data in a distributed ledger.

Identification of nodes in the network takes place by means of decentralized identifiers (DIDs). A DID is essential for participating in the network and doing transactions. This is the number, name or string by which someone is identified. A cryptographic identifier (CID) is a DID that is cryptographically linked to a certain private key.

Most identity-based solutions today have limited support for control over identity, transparency and portability, because third party providers with proprietary systems facilitate such solutions. A fully compliant identity system may not exist in the near future, but this does not preclude the need to establish the founding principles of sovereignty.

In order to enable SSI, a new wave of decentralized identity management protocols and solutions are being standardized as discussed in clauses B.2.1 to B.2.5.

B.2.1 Decentralized identifiers

DIDs are IDs for verifiable, decentralized identity systems including self-sovereign digital identity. In general, DIDs are user generated and self-owned. DIDs possess unique characteristics, which provide greater assurance of immutability and are tamper resistant. DIDs are fully under the control of the DID subject, independent from any centralized registry, IdP, or certificate authority. DIDs are uniform resource locators (URLs) that relate a DID subject to means for trustable interactions with that subject.

In general, DIDs fall into two classes: public DIDs and pairwise DIDs (think of them as semi-private).

1) Public DIDs are IDs used by those users that choose to link themselves with data intended for sharing by the public. Examples include public profiles on social media or verification of a profession such as medical doctor. Public DIDs allow users to support activities that they deem appropriate to share with others and verifiable by others. For example, I can verify that my own personal doctor owns a DID. Public DIDs are traceable and linkable across the Internet.

2) Pairwise DIDs are generated as part of a relationship or set of interactions, whereby users would like to engage in mutual transactions. Pairwise DIDs isolate users and prevent correlation. For the majority of users, pairwise DIDs will be the primary mechanism to conduct identity-based interactions.

DIDs resolve to DID documents, which are simple documents that describe how to use that specific DID. Each DID document contains at least three things: cryptographic material; authentication suites; and service endpoints. Cryptographic material combined with authentication suites provide a set of mechanisms to authenticate a DID subject (e.g., public keys and pseudonymous biometric protocols). Service endpoints enable trusted interactions with the DID subject.

To use a DID with a particular distributed ledger or network requires defining a DID method in a separate DID method specification. A DID method specifies a set of rules for how a DID is registered, resolved, updated and revoked on that specific ledger or network.

This design eliminates dependence on centralized registries for IDs as well as centralized certificate authorities for key management – the standard pattern in a hierarchical public key infrastructure (PKI). Because DIDs reside on a distributed ledger, each entity may serve as its own authority.

Note that DID methods may also be developed for IDs registered in federated or centralized IdM systems. For their part, all types of ID system may add support for DIDs. This creates an interoperability bridge between the worlds of centralized, federated and decentralized identifiers.

B.2.2 Identity hubs

Identity hubs (IHs) are the components responsible for storing identity assertions about subjects. IHs are based on a decentralized model to store semantic representations of any object and expose them as specific URLs. An IH architecture can bring together identities stored on different providers ranging from cloud directories to devices.

B.2.3 Universal decentralized identifier resolver

A universal DID resolver acts like a distributed system that can resolve DIDs on multiple DLT or blockchains. A universal DID resolver has a similar purpose to the binding mechanism in a domain name system system. Instead of working with domain names, universal DID resolvers focus on addressing SSIs that can be created and registered directly by the entities they refer to. The concept is depicted in Figure B.1.

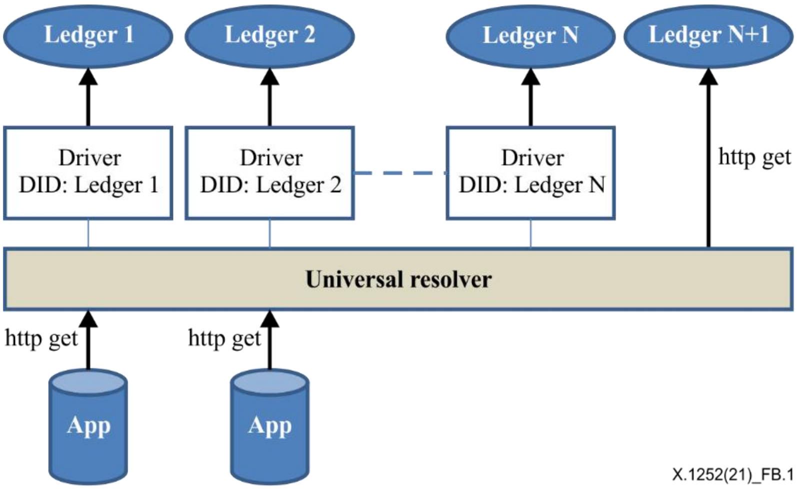


Figure B.1 – Universal DID resolver

B.2.4 Verifiable credentials

Verifiable claims are useful when an entity needs to prove that they are:

- above a certain age;
- capable of driving a particular motor vehicle;
- require a particular medication;
- trained and certified as an electrician;
- professionally licensed to practice medicine; and
- cleared to travel internationally.

The verifiable claims ecosystem is composed of four primary roles.

1) The issuer, who issues verifiable credentials about a specific subject.

2) The holder stores credentials on behalf of a subject. Holders are typically also the subject of a credential.

3) The verifier requests a profile of the subject. A profile contains a specific set of credentials. The verifier verifies that the credentials provided in the profile are fit for purpose.

4) The ID registry is a mechanism that is used to issue IDs for subjects.

Figure B.2 is a visual depiction of the ecosystem.

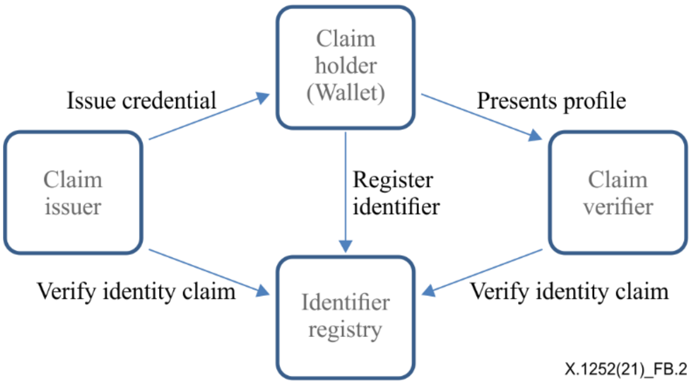


Figure B.2 – The ecosystem

B.2.5 Decentralized wallet

In this model, a user can access a service by presenting their ID to the service provider (RP) in the form of a token. The RP verifies the identity by comparing the hash values of IDs with their corresponding hash records in the DLT. The RP grants or refuses access based on the verification result. In more advanced scenarios, the user can derive separate key pairs from a master private key to generate separate IDs for different relationships to enable privacy friendly interactions.

Figure B.3 depicts the overall identity interactions in support of an identity-based service. The Figure depicts the following steps in decentralized identity transactions:

- A user decides to interact using the decentralized identity services of an identity trust fabric. As depicted in the decentralized ledger box in Figure B.3, the DLT provides services to enable the end user to establish a DID and a relationship with the ledger. The task of establishing a DID for the user results in saving a ledger address for that user and the creation of public-private key pairs for interactions with the user. The ledger also maintains the DID document and establishes the required JavaScript object notation for linked data links as specified by the user. The ledger provides core identity services that enable services to discover how to interact with the user wallet in order to query available claims under user control.
- The creation of a DID on the ledger leads to the creation of a wallet to be used by the user to provide verified claims to the RP. The wallet holds user private keys, public keys and other identity profiles as needed by the DID. The use of zero knowledge techniques ensures that claims can be verified in a manner that preserves privacy and in line with current usage of traditional paper-based credentials and documents. For example, a user can prove their age with a driving licence at a restaurant without the need for the issuer to participate in the transaction. The required steps are provided in the following paragraphs. The wallet can be virtual, where one part of the wallet is on the user mobile device and another in the cloud. This configuration enables the creation of agents to act on behalf of the user and perform services without the need for user direct involvement.

    1) DID registration: the user downloads the wallet that is associated with the DLT core service provider and registers their DID on the ledger. The DLT generates the private and public key pairs for the identity wallet. In addition, a location or address is created and stored on the DLT as part of the registration process.

    2) Identity initiation: For a DLT to be used in decentralized identity systems, a trust framework is assumed to specify the set of available identity services for the participants. In this regard, a user can rely on the availability of an issuer (a trusted party) that can validate the identity of the services. Users can build on the initial claims to collect claims from multiple providers to include in their wallet and enhance their identity validity within the system. From Figure B.3, every relationship is protected by mutual DID between the issuer, the holder (user) and the verifier.

    3) Verification: If a holder (user) wants to access a service from an RP, the RP (verifier) will query the user about available claims. The verifier then consults the ledger to validate the signed claims by using the public keys that correspond to the DID and relate to the transaction. This step includes other layers of authentication. In particular, the way the system works, it is assumed that the wallet is the source of truth in terms of knowing the holder private keys. The system assumes that appropriate authentication has occurred to ensure that the legitimate wallet owner is the entity that is performing the transaction.

    4) Claim validation: The RP uses the claims provided by the wallet to verify the user identity and attribute-using PKI-based signature, as well as hash validation techniques.

    5) Authorization: The RP determines which services can be accessed based on the results of identity verifications.

- DID design calls for the ability of a universal resolver of any DID. This requirement is still work in progress from the DLT community. In decentralized identity models, there is a need to establish an interoperable DID authentication layer. This is still work in progress.

- DID authentication enables an identity owner to prove control over a DID during its interaction with an RP. This requires the following steps to be executed by the RP:

  1) the RP resolves the identity owner's DID to a DID document;
  2) the RP attempts to authenticate the identity owner using the authentication object(s) found in the DID document;
  3) the authentication object(s) may include or reference a publicKey object, if the identity owner's proof is established as a cryptographic signature.

- DID authentication must be understood to be extensible with regard to how an identity owner can prove control over a DID.

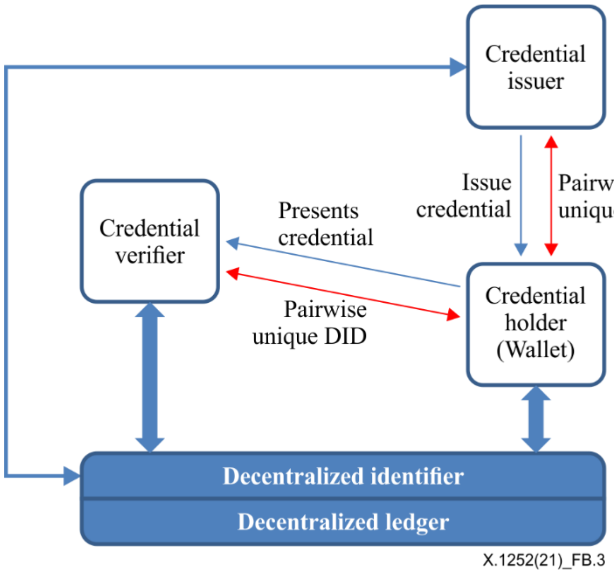


Figure B.3 – Decentralized identity wallet with verifiable claims

Bibliography

[b-ITU-T E.101] Recommendation ITU-T E.101 (2009), *Definitions of terms used for identifiers (names, numbers, addresses and other identifiers) for public telecommunication services and networks in the E-series Recommendations*.

[b-ITU-T L.1410] Recommendation ITU-T L.1410 (2014), *Methodology for environmental life cycle assessments of information and communication technology goods, networks and services*.

[b-ITU-T X.501] Recommendation ITU-T X.501 (2019) | ISO/IEC 9594-2:2020, *Information technology – Open Systems Interconnection – The Directory: Models*.

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

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

[b-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*.

[b-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*.

[b-ITU-T X.1254] ITU-T X.1254 (2020), *Entity authentication assurance framework*.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T X.1403] Recommendation ITU-T X.1403 (2020), *Security guidelines for using distributed ledger technology for decentralized identity management*.

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

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

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

[b-ISO/IEC 2382-37] ISO/IEC 2382-37:2017, *Information technology — Vocabulary — Part 37: Biometrics*.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2019, *IT Security and Privacy – A frame work for identity management – Part 1: Terminology and concepts*.

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information Technology – Security techniques – Entity authentication assurance framework*.

[b-OIX-TFIS] Makaay, E., Smedinghoff, T., Thibeau, D. (2017). *Trust frameworks for identity systems*, White paper, Trust framework series. London: Open Identity Exchange. 18 pp. Available [viewed 2021-05-17] at: https://connectis.com/wp-content/uploads/2018/05/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

[b-W3C-DIDs] W3C (Internet), [Untitled], Decentralized identifiers (DIDs) … Cambridge, MA: World Wide Web Consortium. Available [viewed 2021-05-15] at: https://w3c.github.io/did-core/

[b-W3C-VC] W3C Working Group Note (2019), *Verifiable credentials use cases*. Cambridge, MA: World Wide Web Consortium. Available [viewed 2021-05-17] at: http://www.w3.org/TR/vc-use-cases/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021