

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

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

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/>.

© ITU 2021

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
4	Abbreviations and acronyms	1
5	Conventions	2
6	Terms and definitions	2
	Annex A – Key points and rationale for identity management basic terminology.....	9
	A.1 Authentication and confidence	9
	A.2 Claim or assertion.....	13
	A.3 Enrolment and registration	13
	A.4 Identity provider and identity service provider	14
	A.5 Identity pattern.....	14
	Annex B – Key points and rationale for decentralized identity management basic terminology.....	16
	B.1 Decentralized identity.....	16
	B.2 Decentralized identity model.....	16
	Bibliography.....	22

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



Documents

Document Sharing Hub

Rec. ITU-T X.1252 (04/2021)

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 proofs, 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.