

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1255

(09/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Framework for discovery of identity management information

Recommendation ITU-T X.1255



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
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

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

Recommendation ITU-T X.1255

Framework for discovery of identity management information

Summary

The purpose of Recommendation ITU-T X.1255 is to provide an open architecture framework in which identity management information can be discovered. This IdM information will necessarily be represented in different ways and supported by various trust frameworks or other IdM systems using different metadata schemas. This framework will enable, for example, entities operating within the context of one IdM system to have identifiers from other IdM systems accurately resolved. Without the capability for discovering such information, users and organizations (or programs operating on their behalf) are left to determine how best to establish the credibility and authenticity of a suitable identity, whether for a user, a system resource, information or other entities. Based on this information, it is up to the user or organization to determine whether or not to rely on a given trust framework or other IdM system for such purposes. The core components of the framework set forth in this Recommendation include: 1) a digital entity data model, 2) a digital entity interface protocol, 3) one or more identifier/resolution systems and 4) one or more metadata registries. These components form the basis of the open architecture framework.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1255	2013-09-04	17

Document released under CC BY-SA 4.0

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2013

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
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Conventions	3
6	Recommendation	3
	6.1 Notions of trust	4
	6.2 Trust information.....	4
	6.3 Federated registries for discovery	5
7	Interoperability architecture for federated registries	7
	7.1 Digital entity data model	7
	7.2 Digital entity interface protocol.....	10
	7.3 Interactions with a registry	11
	7.4 Resolution systems	12
	7.5 Distributed queries and aggregated metadata in federated registries	12
	7.6 Metadata schemas.....	15
	7.7 Metadata interoperability.....	15
8	Types and type attributes	15
9	Hierarchical federation and peer-to-peer federation.....	17
	Appendix I – Scenarios of usage.....	20
	Appendix II – BNF notation for a Type record	24
	Bibliography.....	26

Recommendation ITU-T X.1255

Framework for discovery of identity management information

1 Scope

Discovery of identity management information deals with the fact that one must have the ability to obtain relevant information about identifiers, including those utilizing e-mail address syntax and those that are URLs, as well as persistent identifiers. Such discovery is a key element for enabling interoperability across heterogeneous information systems.

The scope of this Recommendation is for a framework that:

- enables the discovery of identity-related information and its provenance, including information being identified such as services, processes and entities;
- enables the discovery of identity-related information attributes including, but not limited to visual logos and human-readable site names;
- enables the discovery of attributes and the functionality of applications;
- describes a data model and a protocol to enable meta-level interoperability for representation, access and discovery of the information referenced above in heterogeneous IdM environments.

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.

[ISO 8601] ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 entity [b-ITU-T Y.2720]: Anything that has a separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices. An entity may have multiple identifiers.

3.1.2 identity provider [b-ITU-T Y.2720]: 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.

3.1.3 relying party [b-ITU-T Y.2720]: An entity that relies on an identity representation or claim by a requesting/asserting entity.

3.1.4 trust [b-ITU-T Y.2720]: A measure of reliance on the character, ability, strength or truth of someone or something.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 association: A relationship, if any, between two identified entities.

3.2.2 digital entity: An entity represented as, or converted to, a machine-independent data structure consisting of one or more elements in digital form that can be parsed by different information systems; the structure helps to enable interoperability among diverse information systems in the Internet.

3.2.3 discovery: The act or process of seeking or locating target information, i.e., obtaining knowledge pertaining to the target.

3.2.4 element: Part of a digital entity consisting of a type-value pair, where the type is represented by a resolvable persistent identifier and the value is the relevant digital information for that type.

3.2.5 federated registries: A collection of interoperable registries that register metadata and participate in a common set of methods to share information reliably and in a commonly understood format.

3.2.6 identifier: A sequence of bits used to obtain state information about the digital entity being identified; typically, this is done via an appropriate resolution system.

3.2.7 identity management: A means by which identity management information, whether for a user, a system resource, information or other entities, can be validated.

3.2.8 identity management information: Identity-related information including all types of metadata associated with identity, provenance, association and trust.

3.2.9 metadata: Structured information that pertains to the identity of users, systems, services, processes, resources, information or other entities.

3.2.10 persistent identifier: A unique identifier that resolves to state information about a digital entity and that is resolvable for at least as long as the digital entity exists.

3.2.11 provenance: Information pertaining to any source of information including the party or parties involved in generating it, introducing it and/or vouching for it.

3.2.12 registry: A mechanism for registering metadata about digital entities and storing metadata schemas, and which provides an ability to search the registry for persistent identifiers based on the use of the metadata schemas.

3.2.13 repository: An interface that accepts deposits of digital entities, enables their retention, and provides secure access to the digital entities via their identifiers.

3.2.14 resolution system: A system that accepts identifiers known to the system as input, and provides relevant state information about the entity being identified.

3.2.15 touch point: A registry within a system of federated registries that is selected to interface with a designated registry in another federation, typically for the purposes of peering.

3.2.16 trust framework: An IdM system where a set of verifiable commitments are made by each of the various parties in a transaction to their counter parties, and these commitments necessarily include: (a) controls to help ensure commitments are met and (b) remedies for failure to meet such commitments.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Program Interface
Bits	Binary Digits
BNF	Backus Normal Form
DE	Digital Entity
DEIP	Digital Entity Interface Protocol
DNA	Deoxyribonucleic acid
HTTP	Hypertext Transfer Protocol
ID	Identifier
IdM	Identity Management
IdP	Identity Provider
MAC	Media Access Control
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
RP	Relying Party
TCP	Transmission Control Protocol
TF	Trust Framework
URL	Uniform Resource Locator
XML	Extensible Markup Language

5 Conventions

None.

6 Recommendation

This Recommendation is for an open architecture framework to support the discovery of identity management information. It addresses the following subjects:

- a) the concept of trust, which is an important aspect of identity management;
- b) trust information, which may be used to determine how much reliance to place on any piece of IdM information;
- c) federated registries for discovery;
- d) an interoperability architecture for federation; and
- e) a discussion of both hierarchical and peer-to-peer federations.

Discovery of identity management information is based on the use of metadata obtained from a registry or a system of federated registries. The framework includes the existence of a means of resolving persistent identifiers. In general, federated registries will be operated by multiple parties and shall support the digital entity data model to represent metadata records and the digital entity interface protocol to achieve the interoperability of such registries. The use of multiple schemas is presumed and each registry shall provide details of its publicly and/or privately supported metadata schemas by their respective persistent identifiers. The persistent identifiers of privately supported

schema may be made known publicly, if desired, or they may be maintained privately along with the associated metadata schemas for limited use within restricted communities.

Appendices I and II respectively provide an overview of scenarios of usage and an example BNF description of a type record (BNF is a standard notation for representing context-free grammars).

6.1 Notions of trust

The word 'trust' is a term of art and carries a number of connotations. To trust a person or process generally means to have some level of confidence in a certain outcome of events, even if those events are not precisely specified. Building discovery systems however, will require added specification. To simply state that A can trust B does not mean that A can trust B for all possible event outcomes. Trusting B to return a service for a given payment is not the same as trusting B to keep that payment secret or to not publicize the names of everyone who makes such payments.

The most important issue in trust frameworks is identity management, that is, are the parties in any given transaction really who they claim to be. But confidence in the outcome of a given transaction with a given party is dependent not only on the identity of that party but also on other attributes of the claims and assertions made by that party. To evaluate these attributes in a consistent fashion requires a vocabulary or set of metrics that can be applied to these attributes. Such measures and descriptions could be applied by third parties serving as trust framework rating agencies, or they could be averaged across groups of ratings from users, as is done in recommendation systems and other 'crowd sourcing' applications. Recommended categories for these measures and descriptions are described below.

Strength: Level of trustworthiness. How likely is this party to do what they say they will do? How likely is it that the assertion of identity (e.g., I am the author of that software and the royalty belongs to me) is correct? This is likely to be expressed as a numeric or letter grade.

Classification: What type of trustworthiness is being asserted? Can standard categories be established? Identity is a category unto itself. Other categories would include financial trustworthiness (e.g., how likely is a given party to perform as promised in a financial transaction), privacy (how likely is a given party to keep private information that it claims will not be released), and authoritativeness (e.g., how likely is it that the information received from a given party is accurate). Other high-level classes are possible and finer levels of granularity are possible for each class.

Length of trust chain: Some trust transactions depend on a chain of trust, frequently thought of in terms of a certificate hierarchy or layers of digitally-signed software. The concept is generally applicable to all areas of trust: the longer the chain of trusted assertions which go back to a trust anchor, the weaker the final level of trust. A measure of the length of this chain would be a key measure of trustworthiness of any identity or other assertion.

All of these attributes (and many others) would be candidates for inclusion in metadata records describing identity providers, relying parties and any other components involved in trusted transactions.

6.2 Trust information

Three distinct aspects of trust information are discussed below in relation to the functions and actions involved in federated discovery and those of the participating constituent entities.

6.2.1 Trust information in a discovery response

Enabling the discovery of identity management information is a primary objective of the open architecture set forth in this Recommendation; however, the determination of trust is left to the user to determine. Additional functionality or services can be supported within the architecture in the form of optional components/modules (software and/or hardware). In this sense, the architecture

could include a trust framework as an optional capability, as well as enhance/enrich a discovery response with trust information or even support a trust determination. External entities would have the ability to determine whether they want to receive this trust information directly. They could choose to deactivate the feature and seek to collect trust information on their own or even from their own sources to make a trust determination.

6.2.2 Trust in the discovery system

The discovery system must be trusted, so that external parties feel confident in using its capabilities to register identity management information or to access it. This type of trust can be achieved through various means, including the establishment of specific methods, along with associated policies and procedures for reliability purposes. These may include evaluation of the components that are implemented as part of the framework, actions (measures) taken for misbehaving components or external parties, and adaptation of strong security and privacy frameworks. However, defining the exact methodology to achieve this kind of trust is outside the scope of this Recommendation.

6.2.3 Trusting external parties

The architecture must support policies and procedures that encourage reliable external parties to use it for the purpose of registering information. For security reasons, component entities that are directly involved in registering identity management information must be able to control the data inserted in the system and detect and/or avoid cases where malicious parties try to register false information.

Anonymous requests should be supported, but many of them may not lead to useful responses unless the identity of the individual requesters is known beforehand through some other means. In such cases, the capability for validating identity should be provided by an identity management capability that applies to all components, including users/requesters. Within the framework, each component is allotted a unique persistent identifier by an authorized and recognized identity provider that can be resolved to relevant information about the component. As indicated earlier, no assumption is made about how any component of a specific instance will determine whether to trust this information.

For many requests, the identity of the requester (an external party that issued a discovery request) must be validated before issuing a response. In the general case, all requesters would be evaluated prior to taking any further action. The architecture does not assume any decision-making capability is invoked within it; however, before constructing the final response to a discovery request, an external decision support mechanism may be invoked in order for permission to be obtained in advance from the identity producers.

6.3 Federated registries for discovery

A system of federated registries for discovery is described in this Recommendation with the goal of enabling metadata and other information about identifiers, as well as trust frameworks and other IdM systems to be found and evaluated. Federated registries can work together to share their metadata entities subject to any restriction that may apply. The actual information which corresponds to this metadata may be stored in their respective registries (if such storage is allowed), in one or more distributed repositories and, in some cases the information corresponding to this metadata may not be accessible in the Internet at all. In the latter case, this limitation would typically be determined by resolving the identifier to relevant state information about the entity; however, a registry could choose to provide that information as well.

Within a system of federated registries, a given registry can contribute a metadata record for a given entity to a second registry either as a full copy of the original metadata record or as a summary of that original record. The submission would have the original record, or a variant of the original, described in such a way that identified from where it was obtained, and which characterized the

