

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1251

(09/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

A framework for user control of digital identity

Recommendation ITU-T X.1251



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

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



Recommendation ITU-T X.1251

A framework for user control of digital identity

Summary

Recommendation ITU-T X.1251 defines a framework to enhance user control and exchange of their digital identity related information. This Recommendation also defines user and functional capabilities of the digital identity information exchange. The work includes providing the user with the ability to control the release of personally identifiable information.

Source

Recommendation ITU-T X.1251 was approved on 25 September 2009 by ITU-T Study Group 17 (2009-2012) under the WTSA Resolution 1 procedure.

Keywords

Digital contract, digital identity, digital identity client, identity, identity interchange, identity management, identity server.

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 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 2010

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

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Terms and 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	General capabilities	4
6.1	User capabilities	4
6.2	Functional capabilities.....	4
6.3	Security guidelines	5
7	Enhanced user control of digital identity interchange	5
7.1	Introduction	5
7.2	Security threats	6
7.3	Conceptual model for digital identity interchange	6
7.4	Digital contract	8
7.5	Three layers for identity interchange.....	9
8	Digital identity interchange framework.....	10
8.1	Design principles	10
8.2	Framework components	11
Appendix I – Reference implementation guideline for a framework for user control of digital identity using WS-trust and Information Card technology		14
I.1	Introduction	14
I.2	Background.....	14
I.3	DIIF capabilities	15
Bibliography.....		18

Recommendation ITU-T X.1251¹

A framework for user control of digital identity

1 Scope

This Recommendation defines a framework to enhance user control and exchange of their digital identity related information.

This Recommendation also defines capabilities for the digital identity information exchange. The work includes providing the user with the ability to control the release of personally identifiable information.

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.

[ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

[ITU-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.2 entity [b-ITU-T X.1252]: Anything that has separate and distinct existence and that can be identified in context.

NOTE – 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 individuals. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

3.1.3 federation [b-ITU-T X.1252]: An association of users, service providers and identity service providers.

3.1.4 identifier [b-ITU-T X.1252]: One or more attributes used to identify an entity within a context.

¹ This Recommendation may not be applicable in some countries due to their domestic legislation.

3.1.5 identity [b-ITU-T X.1252]: The representation of an entity in the form of one or more information elements which allow the entity(s) to be sufficiently distinguished within 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.

NOTE – Each entity is represented by one holistic identity, which 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.

3.1.6 identity management [b-ITU-T Y.2720]: 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 (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects); and
- enabling business and security applications.

3.1.7 identity service provider (IdSP) [b-ITU-T X.1252]: An entity that verifies, maintains, manages, and may create and assign identity information of other entities.

3.1.8 personally identifiable information (PII) [b-ITU-T Y.2720]: The information pertaining to any living person which makes it possible to identify such individual (including the information capable of identifying a person when combined with other information even if the information does not clearly identify the person).

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

3.1.10 user [b-ITU-T X.1252]: Any entity that makes use of a resource e.g., system, equipment, terminal, process, application, or corporate network.

3.1.11 user-centric [b-ITU-T X.1252]: An IdM system that can provide the (IdM) user with the ability to control and enforce various privacy and security policies governing the exchange of identity information, including PII, between entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 circle of trust: A set of criteria established for joining organizations within a federation for the purposes of trusted access to each other's resources. Note that a circle of trust is also the end result of joining organizations within a federation.

3.2.2 digital contract: A contract made in digital form and signed by two entities between whom an agreement is reached.

3.2.3 digital identity: The digital representation of the information known about a specific individual, group or organization.

3.2.4 digital identity client: A client program that provides authentication and credential management, identity interchange and privacy protection service to the user.

3.2.5 identity fraud: A crime in which an impostor obtains key pieces of personally identifiable information (PII) such as social security numbers and driver's license numbers and uses them for his own personal gain.

3.2.6 identity information: The information identifying a user, including trusted (network generated) and/or untrusted (user generated) addresses.