

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1250

(09/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Baseline capabilities for enhanced global identity management and interoperability

Recommendation ITU-T X.1250

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.1250

Baseline capabilities for enhanced global identity management and interoperability

Summary

Recommendation ITU-T X.1250 describes baseline capabilities for global identity management (IdM) interoperability (i.e., to enhance exchange and trust in the identifiers used by entities in telecommunication/information technology IT networks and services). The definitions and need for IdM are highly context-dependent and often subject to very different policies and practices in different countries. The capabilities include the protection and control of personally identifiable information (PII).

Source

Recommendation ITU-T X.1250 was approved on 25 September 2009 by ITU-T Study Group 17 (2009-2012) under the WTSA Resolution 1 procedure.

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 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	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations.....	3
5	Conventions	4
6	General.....	4
7	Capabilities for global identity management and interoperability	5
7.1	Examples of possible identity management transaction models	5
7.2	An interoperable set of identity management (IdM) capabilities.....	8
7.3	Four basic identity components.....	9
7.4	Discovery of identity capabilities.....	11
7.5	Interoperability and bridging	12
7.6	IdM security.....	13
7.7	Protection, control and use of personally identifiable information (PII).....	14
7.8	Auditing and compliance.....	15
7.9	Performance, reliability and availability	16
7.10	Internationalization.....	16
	Bibliography.....	17

Document ID: 123456789

Recommendation ITU-T X.1250¹

Baseline capabilities for enhanced global identity management and interoperability

1 Scope

This Recommendation describes baseline capabilities for enhancing global identity management and interoperability using public telecommunication networks and services. These baseline capabilities are grouped into functional areas:

- Common, structured identity management models.
- Provision of attributes (including identifier), credential and capabilities.
- Discovery of identity service provider resources, capabilities, and federations.
- Interoperability among management platforms, identity service providers and provider federations, including identity service bridge providers.
- Security and other measures to mitigate identity threats and risks, including protection of identity resources, personally identifiable information and privacy.
- Auditing and compliance, including policy enforcement and protection of personally identifiable information.
- Performance, reliability, and availability of identity management capabilities.

Today's telecommunication/IT networks and services are very diverse, highly distributed, highly interconnected, yet substantially autonomous in identity management (IdM). While these networks and capabilities are evolving, their size and complexity may inhibit interoperability among IdM capabilities. For this reason, IdM capabilities in this Recommendation rely substantially on existing network capabilities and general models – including what are effectively best practices. However, to achieve global identity management and interoperability, this Recommendation describes an evolution path and how to build on existing capabilities, where possible. It also defines an identity bridge capability that can be employed in many IdM systems and support architectures to integrate existing IdM capabilities.

The implementation of IdM capabilities in individual countries is subject to requirements specific to the national jurisdiction.

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

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 claimant [b-ITU-T Y.2720] and [b-ITU-T X.811]: An entity which is or represents a principal for the purposes of authentication. A claimant includes the functions necessary for engaging in authentication exchanges on behalf of a principal.

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

3.1.2 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).

3.1.3 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.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 agent: An entity that acts on behalf of another entity.

3.2.2 anonymity: The property that an entity cannot be identified within a set of entities.

NOTE – Anonymity prevents the tracing of entities or their behaviour such as user location, frequency of a service usage, and so on.

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

3.2.4 authentication: See entity authentication.

3.2.5 authentication assurance: Confidence reached in the authentication process that the communication partner is the entity which it claims to be or is expected to be.

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

3.2.7 claim: An assertion made by a claimant of the value or values of one or more identity attributes of a digital subject, typically an assertion which is disputed or in doubt.

3.2.8 entity: 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, a software application, a 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.

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

3.2.10 federation: An association of users, service providers and identity providers.

3.2.11 identifier: One or more attributes used to identify an entity within a context.

3.2.12 identity: 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.

3.2.13 identity service bridge provider: An identity service provider that acts as an intermediary among other identity service providers.