



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1253

(09/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Security guidelines for identity management systems

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/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 2011

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

Draft new Recommendation ITU-T X.1253 (X.idmsg), Security guidelines for identity management systems

Summary

This Recommendation proposes security guidelines for identity management (IdM) systems. The security guidelines provide how an IdM system should be deployed and operated for secure identity services in NGN (Next Generation Network) or cyberspace environment. The security guidelines focus on providing official advice how to employ various security mechanisms to protect a general IdM system and it also provides proper security procedures required when two IdM systems are interoperated.

Table of Contents

1	Scope	4
2	References.....	4
3	Terms and definitions	4
3.1	Terms defined elsewhere	4
3.2	Terms defined in this Recommendation.....	5
4	Abbreviations and acronyms	6
5	Conventions	6
6	Introduction	6
7	Overview of identity management system	7
7.1	General model of IdM system	7
7.2	Identity services.....	7
8	Security threats in IdM system	8
8.1	Systems security	8
8.2	Passive security threats.....	9
8.3	Active security threats	9
8.4	IdM system related security threats.....	10
9	Security guidelines for IdM system.....	11
9.1	Security guidelines for deployment of IdM systems	11
9.2	Security guidelines for operation of IdM systems.....	12
9.3	Security guidelines for IdM servers	12
9.4	Security guidelines for IdM clients	14
9.5	Security guidelines for mobile IdM clients	14
9.6	Privacy considerations in IdM systems	15
	Bibliography.....	17

Recommendation ITU-T X.1253

Security guidelines for identity management systems

1 Scope

The scope of this Recommendation is as follows:

- General IdM system models and services
- IdM system related security threats and risks
- Security guidelines for deployment of IdM systems
- Security guidelines for operation of IdM systems
- Privacy considerations in IdM systems

The scope of this Recommendation mainly focuses on multi-domain based identity management services. However the guideline is also applicable for the centralized identity management system.

Note: Implementers and users of the described guidelines shall comply with all applicable national and regional laws, regulations and policies. Some specific regulation and legislation may require implementation of mechanisms to protect personally identifiable information.

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.

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

[ITU-T X.1252] Recommendation ITU-T X.1252, *Baseline identity management terms and definitions*.

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [ITU-T X.1252]: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.2 attribute [ITU-T X.1252]: Information bound to an entity that specifies a characteristic of the entity.

3.1.3 (entity) authentication [ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

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

3.1.5 entity [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.

3.1.6 identity [ITU-T X.1252]: The representation of an entity in the form of one or more information elements which allow the entities 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.

3.1.7 identity management [ITU-T X.1252]: 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
- supporting business and security applications.

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

3.1.9 user-centric [ITU-T X.1252]: An identity management (IdM) system that provides the user with the ability to control and enforce various privacy and security policies governing the exchange of identity information, including the users personally identifiable information (PII), between entities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 IdM client: The client program that interact with IdM server to retrieve identity information.

3.2.2 IdM server: The server that manages the lifecycle of identity for a user.

3.2.3 Mobile IdM client: IdM client that is installed and used in a mobile device.