International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 7
(02/2009)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1250 series – Supplement on overview of identity management in the context of cybersecurity

ITU-T X-series Recommendations – Supplement 7

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.

Supplement 7 to ITU-T X-series Recommendations

ITU-T X.1250 series – Supplement on overview of identity management in the context of cybersecurity

Summary

The security of the traditional public circuit switched telephone network (PSTN) has been addressed over many decades of operation. However, the same cannot be said for distributed public packet-switched networks with multiple-service providers, such as the Internet and next generation networks (NGNs). Such networks use one common transport platform for control traffic and for user traffic which, in addition to the possible anonymity of such traffic and the possibility of generating unidirectional traffic, makes such networks vulnerable to misuse. All electronic services (e-services such as e-business, e-commerce, e-health, e-government) are open to attack. This problem can be at least partly addressed by improving confidence in the identity of users, network devices and service providers, so that they can be authenticated, granted appropriate access, and audited. Because identity management provides greater assurance and trust in user, service provider, and network device identities, it improves security by reducing exposure to security risks. This aspect of cybersecurity is something that service providers need to consider at a business and technical level, and that governments need to consider on a national level as part of the national cybersecurity plan.

Source

Supplement 7 to ITU-T X-series Recommendations was agreed on 20 February 2009 by ITU-T Study Group 17 (2009-2012).

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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/.

CONTENTS

Page

1 Scope 1

2 References........ 1

3 Definitions 1

4 Abbreviations and acronyms 1

5 Conventions 1

6 Importance of IdM to global network infrastructure protection and multi-national coordination for security........ 1

7 Identity management as an enabler of trusted communication between two entities... 1

8 Protection, maintenance, revocation and control of identity data 2

9 "Discovery" of trusted sources of identity data 2

10 Electronic government services (e-government services) 2

11 Regulatory considerations in connection with IdM........ 2

Introduction

Identity management (IdM) is a way to manage and control the information that is used in the communications process to represent entities (such as service providers, end-user organizations, people, network devices, software applications and services). A single entity may have multiple digital identities in order to access various services with differing requirements, and these may exist in multiple locations.

IdM is a key component of cybersecurity because it provides the capability to establish and maintain trusted communications among entities. IdM supports authentication of an entity. It also enables the authorization of a range of privileges (rather than all-or-nothing privileges) and makes it easier to change privileges if an entity's role changes. IdM also improves an organization's ability to apply its security policies by enabling an entity's activity on the network to be monitored and audited. IdM can provide access to entities both inside and outside an organization. In short, a good IdM solution provides capabilities to support authentication, provision and manage identities, and audit an entity's activities.

IdM is a critical component in managing security and enabling nomadic, on-demand access to networks and e-services. Along with other defensive mechanisms (e.g., firewalls, intrusion detection systems, virus protection), IdM plays an important role in protecting information, communications and services from cybercrimes such as fraud and identity theft. One consequence of this is that users' confidence will grow as e-transactions will be secure and reliable. In turn, this will increase users' willingness to use IP networks for e-services.

In implementing an IdM system, fundamental privacy concerns must be addressed. This means developing methods to ensure that identity information is accurate and to prevent identity information from being used for purposes beyond those for which it was collected.

Supplement 7 to ITU-T X-series Recommendations

ITU-T X.1250 series – Supplement on overview of identity management in the context of cybersecurity

1 Scope

Identity management has emerged as a critical component that will improve security by providing greater assurance by verifying the validity of identity information. This supplement provides a general overview of this new service.

The use of the term "identity" in this supplement relating to IdM does not indicate its absolute meaning. In particular, it does not constitute any positive validation.

2 References

None.

3 Definitions

Definitions can be found in other ITU-T Recommendations of the X.1250 series.

4 Abbreviations and acronyms

This supplement uses the following abbreviations:

IdM	Identity Management
IP	Internet Protocol
PSTN	Public Switched Telephone Network

5 Conventions

None.

6 Importance of IdM to global network infrastructure protection and multi-national coordination for security

Proper implementation and use of IdM capabilities and practices in various national, regional, and international networks will enhance the security of the global network infrastructure. IdM best practices and implementations are important and necessary to provide assurance of identity information and of the integrity and availability of the global network infrastructure.

IdM capabilities can be used to support national and international emergency telecommunication services by identifying users authorized for special services.

In addition, IdM capabilities can be used to prevent, detect, and support coordination of responses to national and international cybersecurity incidents. In some instances, IdM may help authorities and entities coordinate their efforts to trace and locate the source of such incidents.

7 Identity management as an enabler of trusted communication between two entities

One important function of IdM is the authentication of users, networks or services. In an authentication process involving two entities, one entity makes assertions about its identity to the other. Depending on the second entity's security requirements, these assertions may need to be validated before the second entity will trust the first enough to grant it privileges. This process may be required in both directions.

There are various levels of authentication trust ranging from little-or-none, weak (e.g., user name and password), to strong (e.g., public key infrastructure (ITU-T X.509)). A risk assessment can identify the appropriate level of authentication. There may need to be higher levels of authentication for one entity than for the other, for example, because one entity controls critical resources.

8 Protection, maintenance, revocation and control of identity data

Other important functions of IdM are to protect, maintain, and control trusted identity data, including the ability to ascertain the current status of an identity.

Laws or policies may require that personally identifiable information is protected and that identity information is prevented from being used for purposes beyond those for which it was collected. Ensuring that identity data continues to be valid is another primary concern. For the services that use them to be viable, identity data must be properly maintained so that it is accurate, timely and consistent.

Where relevant, management of identity data attributes should include the capability to check the identity data to see if it has been revoked.

In many cases, entities will want to control the use of their own data and private information.

9 "Discovery" of trusted sources of identity data

IdM also encompasses the concept of "discovery" of trusted identity data. In a highly distributed, multi-provider environment (such as the Internet and next generation networks), identity data necessary to provide trust in the identity and related assertions of an entity can be located in different places on the network. Entities may have multiple digital identities with different sources of identity information in different locations. When one of the two entities in an authentication process is nomadic, the other entity will need to locate and establish a trust relationship with an appropriate source of identity information in order to complete the process of authenticating the nomadic entity. The concept of discovery of sources of trusted information is similar to what occurs today in mobile cell phone usage.

10 Electronic government services (e-government services)

The advantages of an entity to implement IdM include risk reduction, trust enhancement, increased functionality and the potential for cost reduction. These reasons for implementing IdM are equally valid when the entity is a government. In e-government services, the main objectives are also to cut costs and to provide more efficient and more effective services to the government's citizens and business partners.

Like other entities, governments are confronted by the challenge of how to effectively and efficiently utilize identity in the networked world. In order to make e-government services a reality, a government must perform risk analyses on the e-services it intends to offer and implement suitable protective measures. The sensitive nature of many e-government services (for example, e-health) may require a government to require strong authentication.

11 Regulatory considerations in connection with IdM

National administrations and regional groups need to consider a number of potential regulatory issues in connection with IdM implementation, such as privacy and data protection, national security and emergency preparedness, and mandatory settlements between carriers. Governments not only utilize identity management techniques but may also impose it on other entities to meet a broad array of national policy and security objectives.

Selected list of activities related to Identity Management

Various forums are working on IdM issues. These include:

- ARK (California Digital Library Archival Resource Key): http://www.cdlib.org/inside/diglib/ark/(ARK)
- 3GPP SA3: http://www.3gpp.org/tb/sa/sa3/ToR.htm
- ETSI TISPAN WG7: http://www.etsi.org/tispan/
- EU eID Roadmap: http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf
- European Citizen Card: http://europa.eu.int/idabc/servlets/Doc?id=19132
- FIDIS (EU Future of Identity in the Information Society): http://www.fidis.net/
- FIRST (Forum of Incident Response and Security Teams): http://www.first.org/
- Guide project (EU Government User Identity for Europe): http://www.guide-project.org
- Handle: http://www.handle.net/
- Higgins: http://www.eclipse.org/higgins/index.php
- IDSP (American National Standards Institute Identity Theft Prevention and Identity Management Standards Panel (IDSP)): http://www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3
- IGF (ORACLE Identity Governance Framework): http://www.oracle.com/technology/tech/standards/idm/igf/index.htm; see Liberty Alliance
- ITRC (Identity Theft Resource Center): http://www.idtheftcenter.org/
- Internet Engineering Task Force: http://sec.ietf.org/
- ITU-T Study Group 17 (Security) Focus Group on IdM: www.itu.int/ITU-T/studygroups/com17/fgidm/index.html
- ITU-T Study Group 17 (Security) Question 10: http://www.itu.int/ITU-T/studygroups/com17/index.asp
- ITU-T Study Group 13 (Future Networks) Question 13: http://www.itu.int/ITU-T/studygroups/com13/index.asp
- Liberty Alliance Project: http://www.projectliberty.org/
- Light Weight Identity: http://lid.netmesh.org/wiki/Main_Page
- MODINIS-IDM Consortium: http://www.egov-goodpractice.org and https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium
- National Identity Card Schemes: e.g., http://www.identitycards.gov.uk/index.asp; http://en.wikipedia.org/wiki/Identity_document
- OASIS (Organization for the Advancement of Structured Information Standards): http://www.oasis-open.org/home/index.php
- OECD (Organization for Economic Co-operation and Development) Workshop on Digital Identity. Management in Trondheim, Norway, May 8th-9th 2007: http://www.oecd.org/sti/security-privacy/idm
- OMA (Open Mobile Alliance): http://www.openmobilealliance.org/
- The Open Group: http://www.opengroup.org
- OSIS (Open Source Identity System): http://osis.netmesh.org/wiki/Main_Page
- PAMPAS (EU Pioneering Advanced Mobile Privacy and Security (PAMPAS)): http://www.pampas.eu.org/

- PERMIS (EU Information Society Initiative in Standardization (ISIS) PrivilEge and Role).
- Prime (EU Privacy and Identity Management for Europe): https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium – PRIME
- W3C (World Wide Web Consortium): http://www.w3.org/
- Yadis: http://yadis.org/wiki/Main_Page

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009