

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1113

(11/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Guideline on user authentication mechanisms for home network services

ITU-T Recommendation X.1113



International
Telecommunication
Union
Documents

Document Sharing Hub

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

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
TELECOMMUNICATION SECURITY	X.1000–

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

ITU-T Recommendation X.1113

Guideline on user authentication mechanisms for home network services

Summary

Some environments necessitate the authentication of the human user rather than a process or a device. In authenticating human users, the authentication system requires human users to prove their uniqueness. Such uniqueness is generally based on various authentication means such as something known, something possessed or some immutable characteristics for each human user.

In this Recommendation, a guideline on user authentication mechanism for home network services is provided. It also considers various security issues according to ITU-T Recommendation X.1111, which specifies the framework of security technologies for home network. Finally, the security assurance level and authentication model are defined according to authentication service scenarios.

Source

ITU-T Recommendation X.1113 was approved on 13 November 2007 by ITU-T Study Group 17 (2005-2008) under the ITU-T Recommendation A.8 procedure.

Keywords

Authenticated key exchange, client authentication, mutual authentication, security assurance level, server authentication, user authentication, user secrets.

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 2008

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	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Conventions	4
6	Home network architecture.....	5
6.1	General model	5
6.2	Service architecture for user authentication	5
7	Classification of home entities for user authentication.....	6
8	Consideration for user authentication between home entities	7
8.1	Remote terminal (RT) and application server (AS)	8
8.2	Remote terminal (RT) and secure home gateway (SHG).....	8
8.3	Remote terminal (RT) and home application server (HAS).....	8
8.4	Remote terminal (RT) and type A device (HD_A)	8
8.5	Remote terminal (RT) and type B device (HD_B).....	8
8.6	Remote terminal (RT) and type C device (HD_C).....	8
8.7	Type A device (HD_A) and application server (AS)	8
8.8	Type A device (HD_A) and secure home gateway (SHG)	9
8.9	Type A device (HD_A) and home application server (HAS)	9
8.10	Type A device (HD_A) and type B device (HD_B)	9
8.11	Type A device (HD_A) and type C device (HD_C)	9
9	Security threats and security requirements for user authentication mechanisms	9
9.1	Security threats	9
9.2	Resistance against security threats	10
9.3	Security requirements	10
10	User authentication mechanism.....	11
10.1	Scope of user authentication mechanism	11
10.2	Security components of the user authentication mechanism.....	12
10.3	Set-up for the user authentication mechanism.....	14
10.4	Required security services for user authentication between home entities	15
10.5	Security association	16
10.6	Security assurance level	16
10.7	Protection level of SALs	18
10.8	Authentication models.....	18
10.9	Relationship between SAL and home network security requirement	20

	Page
Appendix I – Security association used in IPsec	21
Appendix II – Existing authentication mechanisms	22
Bibliography.....	23

iv

ITU-T Recommendation X.1113

Guideline on user authentication mechanisms for home network services

1 Scope

The goal of this work is to provide a guideline for user authentication mechanisms to enable secure home network services. To this end, this Recommendation first identifies the home entities and their relationships, security threats to the home network and security components to protect the home network from such threats. Likewise, it defines security assurance level and specifies authentication models classified by service access flow to the home network. Finally, the appropriate security assurance level is applied to each authentication model.

Specifically, this Recommendation:

- defines the service architecture for the user authentication mechanisms between the home entities based on the general security framework defined in [ITU-T X.1111];
- describes the classes of home entities applicable to user authentication mechanisms;
- describes the considerations between classes of home entities for user authentication mechanisms;
- identifies the security threats and the functional requirements related to user authentication mechanisms;
- defines the security components of user authentication mechanisms;
- defines the security assurance levels for user authentication, and;
- describes the authentication models.

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 J.190] ITU-T Recommendation J.190 (2002), *Architecture of MediaHomeNet that supports cable-based services*.
- [ITU-T J.192] ITU-T Recommendation J.192 (2004), *A residential gateway to support the delivery of cable data services*.
- [ITU-T X.800] ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.803] ITU-T Recommendation X.803 (1994), *Information technology – Open Systems Interconnection – Upper layers security model*.
- [ITU-T X.810] ITU-T Recommendation X.810 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- [ITU-T X.811] ITU-T Recommendation X.811 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.

Copyright © 2007 ITU-T

- [ITU-T X.814] ITU-T Recommendation X.814 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework.*
- [ITU-T X.815] ITU-T Recommendation X.815 (1995), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework.*
- [ITU-T X.1111] ITU-T Recommendation X.1111 (2007), *Framework of security technologies for home network.*
- [ISO 19092-1] ISO 19092-1:2006, *Financial services – Biometrics – Part 1: Security framework.*

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 administrator of home network:** [ITU-T X.1111]
- 3.1.2 biometric:** [ISO 19092-1]
- 3.1.3 biometric data:** [ISO 19092-1]
- 3.1.4 capture:** [ISO 19092-1]
- 3.1.5 extraction:** [ISO 19092-1]
- 3.1.6 home access:** [ITU-T J.190]
- 3.1.7 home application service provider:** [ITU-T X.1111]
- 3.1.8 home bridge:** [ITU-T J.190]
- 3.1.9 home client:** [ITU-T J.190]
- 3.1.10 home device:** [ITU-T X.1111]
- 3.1.11 home user:** [ITU-T X.1111]
- 3.1.12 ID certificate:** [ITU-T X.1111]
- 3.1.13 match:** [ISO 19092-1]
- 3.1.14 raw biometric data:** [ISO 19092-1]
- 3.1.15 remote terminal:** [ITU-T X.1111]
- 3.1.16 remote user:** [ITU-T X.1111]
- 3.1.17 security console:** [ITU-T X.1111]
- 3.1.18 secure home gateway:** [ITU-T X.1111]
- 3.1.19 template:** [ISO 19092-1]

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

- 3.2.1 authentication server:** Authentication servers refer to servers that provide authentication services to users or other systems. Authentication is generally used as the basis for authorization (determining whether a privilege will be granted to a particular user or process), privacy (preventing the disclosure of information to non-participants), and non-repudiation (not being able to deny having done something that was authorized to be done based on the authentication).

3.2.2 client authentication: Client authentication models a situation in which the server wants to verify the client's identity. The client responds by sending his/her credentials such as digital certificate, shared secret or password.

3.2.3 home portal: A home portal is a functional element that provides management and translation functions to provide the user with home network services such as the control of home devices, multimedia contents, various applications, etc. In general, a home portal is a website that provides a gateway or portal to information related to various home network services. It also allows the home user to maintain and set up his/her home using the Internet. Finally, a home portal is designed to use distributed applications and different numbers and types of middleware and hardware to provide services from a number of different sources. In other words, a home portal offers information to home network services from various home entities in a unified manner.

3.2.4 identity proof: Identity proof refers to a process that a user proves who he/she is. To prove his/her identity in a digital environment, the user uses a set of security credentials such as user name and password, or certificates. For identity proof, those credentials shall include the user's ID corresponding to the user secret. In general, when the user can successfully demonstrate possession and control of a secret token to an authentication system through an authentication protocol, identity proof of the user can be achieved.

3.2.5 implicit authentication: Implicit authentication is a type of authentication without identity proof. Thus, anyone who has the correct secret can access the services.

3.2.6 mutual authentication: Mutual authentication refers to a type of authentication that enables both server authentication and client authentication.

3.2.7 policy database: A policy database refers to a list of policy needs to be created in a file. In the user authentication context, this file defines the rules required for user authentication protocol.

3.2.8 security token: This is a cryptographic key stored in a special hardware device or a general-purpose computing device.

3.2.9 server authentication: Server authentication models a situation in which the client wants to verify the server's identity. The server answers by sending its credentials such as digital certificate or shared secret.

3.2.10 session key: The session key is a temporary key used to encrypt data for the current session only. The use of session keys keeps the secret keys even more secret because they are not used directly to encrypt the data. Secret keys are used to derive the session keys using various methods that combine random numbers from either the client or server or both.

3.2.11 user database: A user database pertains to a list of users and their secrets as created in a file. For security reasons, this file should not be in clear text format. The file consists of a list of usernames and a secret for each user.

3.2.12 user secret: A user secret is a secret key generated by a user itself. A user secret is generally used for providing evidence of the user identity in an authentication mechanism.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AS	Application Server
CA	Certification Authority
CRL	Certificate Revocation List
EAP	Extensible Authentication Protocol
EKE	Encrypted Key Exchange

HAS	Home Application Server
HAVi	Home Audio Video interoperability
HD_A	Type A Home Device
HD_B	Type B Home Device
HD_C	Type C Home Device
ID	Identity or Identifier
IKE	Internet Key Exchange
IPsec	IP Security
Jini	Java intelligent network infrastructure
MITM	Man-in-the-Middle
RT	Remote Terminal
SA	Security Association
SAID	Security Association Identifier
SAL	Security Assurance Level
SHG	Secure Home Gateway
SRP	Simple Retransmission Protocol
TLS	Transport Layer Security
TLV	Type/Length/Value
UPnP	Universal Plug and Play
VPN	Virtual Private Network

5 Conventions

None.