

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1152

(05/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Telecommunication security

Secure end-to-end data communication techniques using trusted third party services

Recommendation ITU-T X.1152

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.



Recommendation ITU-T X.1152

Secure end-to-end data communication techniques using trusted third party services

Summary

Recommendation ITU-T X.1152 defines basic interfaces, interactions and security considerations for secure end-to-end data communication using on-line trusted third party (TTP) services.

This Recommendation also identifies online TTP services which can be used to support secure end-to-end data communication between two entities.

Source

Recommendation ITU-T X.1152 was approved on 29 May 2008 by ITU-T Study Group 17 (2005-2008) under Recommendation ITU-T A.8 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 2009

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.....	3
4	Abbreviations and acronyms	3
5	Convention.....	4
6	TTP services for secure end-to-end data communication.....	4
7	System model	5
8	Processes of a secure end-to-end data communication.....	5
8.1	Establishment phase	5
8.2	Data transmission phase	6
8.3	Termination phase	7
9	Online TTP services to support secure end-to-end data communication	7
9.1	TTP services for establishment phase	7
9.2	TTP services for data transmission phase	8
9.3	TTP services for termination phase.....	9
9.4	Possibilities of online TTP services to support secure end-to-end data communication	9
9.5	Integration of TTP services	9
10	Basic interfaces for secure end-to-end data communication based on online TTP	10
10.1	Requester-TTP interface.....	11
10.2	Responder-TTP interface.....	11
10.3	Requester-Responder interface.....	11
10.4	TTP internal interface.....	11
10.5	Requester internal interface	12
10.6	Responder internal interface.....	12
11	Basic interactions for secure end-to-end data communication based on online TTP...	12
11.1	Preconditions	13
11.2	Establishment of control path.....	13
11.3	Establishment of secure data communication path	14
11.4	Secure data transmission	15
11.5	Audit trail creation.....	16
11.6	Termination of secure data communication path	17
11.7	Termination of control path.....	18
12	Security considerations.....	19
12.1	Requester-TTP interface.....	19

Document Sharing Hub

Documents

Document Sharing Hub

Rec. ITU-T X.1152 (05/2008)

iii

	Page
12.2 Responder-TTP interface.....	19
12.3 Establishment of the secure data communication path between entities.....	19
12.4 Stored data in the entity	19
12.5 Stored data in the TTP.....	19
Annex A – Re-establishment	20
A.1 Re-establishment process of a secure end-to-end data communication	20
A.2 TTP services for re-establishment process	20
Annex B – Entity level granularity and communication level granularity	21
Appendix I – Service scenario	22
Appendix II – Relationship among this Recommendation, ITU-T X.842 and the Liberty Alliance Project	23
Bibliography	24

Recommendation ITU-T X.1152

Secure end-to-end data communication techniques using trusted third party services

1 Scope

This Recommendation defines basic interfaces, interactions and security considerations of online trusted third party (TTP) services for secure end-to-end data communication.

This Recommendation also identifies online TTP services which can be used to support secure end-to-end data communication which is a connection-oriented communication between two entities with no eavesdropping, injection and modification of data, unauthorized access and repudiation.

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 published regularly. 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.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.
- [ITU-T X.842] Recommendation ITU-T X.842 (2000) | ISO/IEC TR 14516:2002, *Information technology – Security techniques – Guidelines for the use and management of trusted third party services*.
- [ITU-T X.1121] Recommendation ITU-T X.1121 (2004), *Framework of security technologies for mobile end-to-end data communications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

- 3.1.1 access control** [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.
- 3.1.2 audit trail** [ITU-T X.800]: Data collected and potentially used to facilitate a security audit.
- 3.1.3 authentication** [b-ITU-T X.811]: The provision of assurance of the claimed identity of an entity.
- 3.1.4 authorization** [ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.
- 3.1.5 availability** [ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.
- 3.1.6 certification service** [b-ITU-T X.843]: The service of creating and assigning certificates performed by a CA.



3.1.7 confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

3.1.8 credentials [ITU-T X.800]: Data that is transferred to establish the claimed identity of an entity.

3.1.9 directory service [b-ITU-T X.843]: A service to search and retrieve information from a catalogue of well defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses, etc. An example is provided by a directory service conforming to Rec. ITU-T X.500.

3.1.10 eavesdropping [ITU-T X.1121]: Anonymous attackers can actively intercept transmitted data, causing a leakage of data.

3.1.11 electronic digital archiving service [ITU-T X.842]: The electronic digital archiving service is a service provided by a document recorder, at which electronic documents are registered for safekeeping and for retention as a permanent record. The archiving of electronic documents in encrypted form may be required in some instances, especially where the data is highly sensitive and requires extra protection.

3.1.12 electronic notary public service [ITU-T X.842]: Notary public services are high level services that make use of a number of basic services such as time stamping, certification, directory service, digital archiving and non-repudiation. In principle a document will be given to the TTP, and the TTP attests or certifies this document by use of digital signatures or some other means. Part of this service may be a directory service, where the information, such as formerly certified documents, may be retrieved from a database or directory.

3.1.13 injection and modification of data [ITU-T X.1121]: This occurs when an unauthorized entity inserts, changes or deletes information transmitted between a mobile terminal and an application server. The unauthorized entity could be a person, a program, or a computer.

3.1.14 integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.15 key distribution service [ITU-T X.842]: The purpose of a key distribution service is to distribute keys securely to authorized entities. Depending on the TTP's security policy, keys may have to be forwarded to other TTP services, e.g. a directory service. These services could be provided by the same or another TTP.

3.1.16 key generation service [ITU-T X.842]: This service is invoked to generate keys in a secure way for a particular cryptographic algorithm.

3.1.17 key management [ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.18 on-line TTP service [ITU-T X.842]: The TTP is involved in all first time secure exchanges between the entities. However, the TTP is not required for follow-up exchanges and is not positioned in the communication path between the entities.

3.1.19 repudiation [ITU-T X.1121]: This attack occurs when a sender or receiver denies the fact of having transmitted or received a message, respectively.

3.1.20 security association [b-ITU-T X.803]: A relationship between two or more entities for which there exist attributes (state information and rules) to govern the provision of security services involving those entities.

3.1.21 security domain [b-ITU-T X.803]: A set of elements, a security policy, a security authority and a set of security relevant activities in which the set of elements are subject to the security policy, administered by the security authority, for the specified activities.

3.1.22 security policy [ITU-T X.800]: The set of criteria for the provision of security services (see also identity-based and rule-based security policy).

3.1.23 time stamping service [ITU-T X.842]: The time stamping service seals a digital document by cryptographically binding a trusted time to it (typically to a hash representation of it called "message digest" or "message imprint"), thus providing a means to detect any modification, such as backdating and avoid replay attacks or other forgeries.

3.1.24 trusted third party [ITU-T X.810]: The trusted third party is an organisation or its agent that provides one or more security services, and is trusted by other entities with respect to activities related to these security services.

3.1.25 unauthorized access [ITU-T X.1121]: This threat occurs when an illegal entity gains access to an application server by masquerading as a real mobile user.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 certified credential: Certified credential is the credential that is authorized by TTP.

3.2.2 control path: Control path is the route between one entity and TTP to control the secure data communication path.

3.2.3 credential mapping service: Credential mapping service is a TTP service that translates an entity's credential for one security domain to the entity's credential for another security domain.

3.2.4 location service: Location service is a TTP service that provides information with regard to the current location of an entity on the network.

3.2.5 peer entity: The peer entity is the entity with which an entity performs secure end-to-end data communication.

3.2.6 policy determination service: The policy determination service is a TTP service that determines security protocols and/or algorithms that are used for data confidentiality and/or data integrity in data transmission phase.

3.2.7 presence service: Presence service is a TTP service that provides availability information of an entity.

3.2.8 secure data communication path: Secure data communication path is the route between two entities to exchange application data between two entities with no eavesdropping, injection and modification of data, unauthorized access and repudiation.

3.2.9 translated credential: Translated credential is a kind of certified credential that belongs to a security domain and is translated from another credential, which belongs to another security domain, by credential mapping service.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

App	Application
CA	Certification Authority
IP	Internet Protocol
MAC	Message Authentication Code
SA	Security Association
SCS	Secure Communication Service

TLS	Transport Layer Security
TTP	Trusted Third Party
URI	Uniform Resource Identifier
VPN	Virtual Private Network

5 Convention

None.

6 TTP services for secure end-to-end data communication

There are various security requirements for data communication as described in [ITU-T X.800], [ITU-T X.805], [ITU-T X.1121] and other security related ITU-T Recommendations. In addition, there are many kinds of security mechanisms/protocols to satisfy these security requirements.

Nowadays, security is an essential and important function for data communication. Basically, each communication layer shall implement necessary security functions. Many designers have designed many secure communication protocols. However, it is inefficient and difficult for all applications to implement all security functions.

Therefore, it is very useful that the network or a trusted third entity on the network (hereafter referred to as "TTP") perform essential (or minimal) security functions on behalf of applications. Although [ITU-T X.842] defines major security services provided by TTP, there is no concrete description as to which TTP services should be used or how to be used when applications perform secure communication.

The purpose of this Recommendation is to define basic interfaces and interactions with online TTP services used for secure end-to-end data communication which is a connection-oriented communication between two entities with no eavesdropping, injection and modification of data, unauthorized access and repudiation. Moreover, this Recommendation also aims to define online TTP services to support the secure end-to-end data communication between two entities.