International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1164

(10/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Peer-to-peer security

Use of service providers' user authentication infrastructure to implement public key infrastructure for peer-to-peer networks

Recommendation ITU-T X.1164

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
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1164

Use of service providers' user authentication infrastructure to implement public key infrastructure for peer-to-peer networks

Summary

Peer entity authentication is a mandatory requirement for securing peer-to-peer communications. However, especially in pure peer-to-peer (P2P) networks, it is difficult for peers to authenticate corresponding peer entities because there is no central server for authentication they can rely on. In addition, the existing public key infrastructure (PKI) has little use for this purpose because those peer entities rarely have public key certificates issued by well-known certification authorities.

The purpose of Recommendation ITU-T X.1164 is to define mechanisms to utilize service providers' user authentication infrastructure to implement PKI for P2P networks, with which users who have a valid e-mail account managed by a service provider can issue certificates to their devices by themselves and make those certificates verifiable by corresponding peers in P2P networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1164	2012-10-14	17

Keywords

Peer entity authentication, P2P, peer to peer, PKI, public key infrastructure.

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/.

Table of Contents

Recommendation ITU-T X.1164

Use of service providers' user authentication infrastructure to implement public key infrastructure for peer-to-peer networks

1 Scope

Recommendation ITU-T X.1164 describes the mechanisms for utilizing service providers' user authentication infrastructure to implement public key infrastructure (PKI) used for securing peer-to peer (P2P) networks. The described mechanisms allow a peer in P2P networks to verify public key certificates, issued by the owner (peer user), of a corresponding peer.

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 X.509] Recommendation ITU-T X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [b-ITU-T X.800]: See data origin authentication [defined in clause 3.1.3], and peer entity authentication [defined in clause 3.1.5].

3.1.2 certificate revocation list (CRL) [ITU-T X.509]: A signed list indicating a set of certificates that are no longer considered valid by the certificate issuer. In addition to the generic term CRL, some specific CRL types are defined for CRLs that cover particular scopes.

3.1.3 data origin authentication [b-ITU-T X.800]: The corroboration that the source of data received is as claimed.

3.1.4 peer [b-ITU-T X.1161]: Communication node on P2P network that functions simultaneously as both "client" and "server" to the other nodes on the network.

3.1.5 peer entity authentication [b-ITU-T X.800]: The corroboration that a peer entity in an association is the one claimed.

3.1.6 peer user [b-ITU-T X.1162]: A peer user is one who uses a computer system to access the P2P network. A peer user in a P2P network is similar to a user in the Internet, with slight differences. Specifically, peer users in the P2P network have a different operational context including personal interests, resource plans, security considerations, etc.

3.1.7 public key certificate (PKC) [ITU-T X.509]: The public key of a user, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority (CA) which issued it.

3.1.8 public key infrastructure (PKI) [ITU-T X.509]: The infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CA	Certification Authority
CRL	Certificate Revocation List
FQDN	Fully Qualified Domain Name
HTTPS	Hypertext Transfer Protocol over Secure Socket layer
P2P	Peer-to-Peer
PDA	Personal Digital Assistant
PKC	Public Key Certificate
PKI	Public Key Infrastructure
S/MIME	Secure Multipurpose Internet Mail Extensions
URL	Uniform Resource Locator

5 Conventions

None.

6 Overview

6.1 Model of peer-to-peer communications between devices of peer users

A model of peer-to-peer communications between devices of peer users is shown in Figure 1.

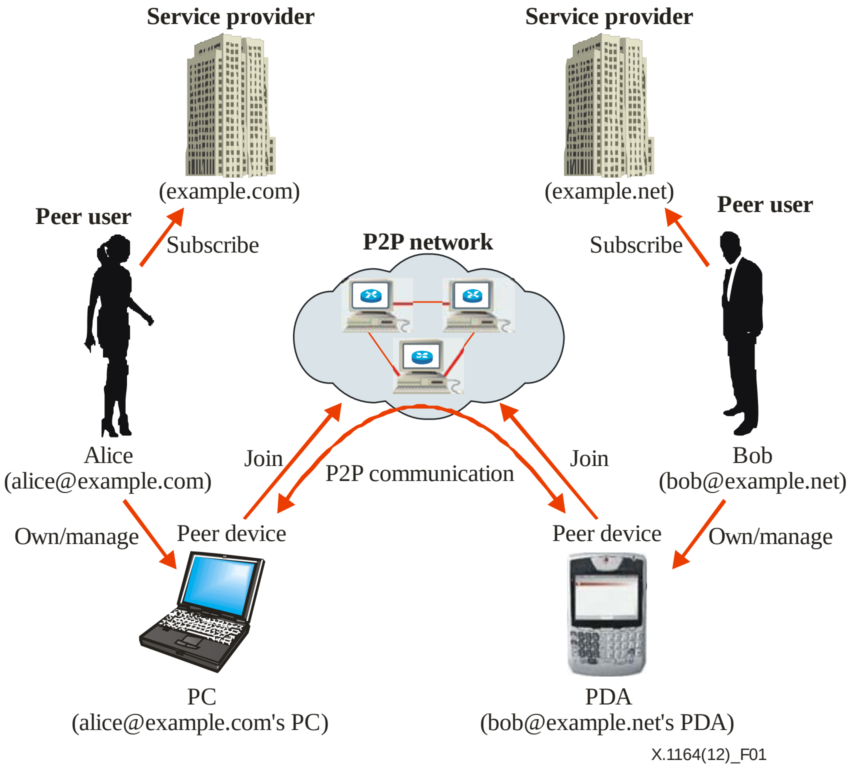

Figure 1 – Model of peer-to-peer communications between devices of peer users

There are four entities in this model: peer user, peer device, service provider and P2P network.

In this model, a peer user is identified by her/his e-mail address and the identity of the peer device is asserted by its owner (peer user). A service provider has the ability to authenticate its users and authorize them to upload their public key information, which can then be consulted by peers in P2P networks and is used for peer entity authentication. The purpose of peer entity authentication in this model is to prove the identity of a corresponding peer and its owner.

6.2 Overview of mechanisms used for implementing PKI for P2P networks

The purpose of the mechanisms described in this Recommendation is to make a public key certificate of a peer device issued by its owner verifiable by anyone. To achieve this, each user acts as a certification authority (CA) for managing public key certificates of her/his own devices. Service providers, then, play the key role in associating users' identity with their CA public key. A service provider which supports the PKI scheme described in this Recommendation has to implement the following two operations.

– Upload of CA certificate and certificate revocation list (CRL) of a user's CA:
  - Authenticate users and authorize them to upload their CA certificate and CRL.

– Retrieval of CA certificate and CRL of a user's CA:
  - Allow anyone to retrieve uploaded CA certificate and CRL in such a way that the binding between the retrieved information and its user's identity (i.e., e-mail address) can be guaranteed.

When utilizing this PKI scheme, a user first generates her/his own CA public key pair and uses it for issuing public key certificates to her/his devices used for P2P networking. The user uses her/his e-mail address as the identity of the certificate issuer. The user, then, uploads the CA certificate and CRL to her/his service provider.

When verifying a certificate of a corresponding peer, a peer retrieves a CA certificate and CRL from the certificate issuer's service provider and uses them to verify authenticity and validity of the certificate.

6.3 Usage scenarios

6.3.1 Building a closed P2P network with friends

By having a member list consisting of e-mail addresses, a P2P network can authenticate joining peers so that only peer devices that are owned by users in the member list will be permitted to join the network.

6.3.2 Access control for P2P resources and services

A peer can implement authentication and authorization mechanisms in order to allow only corresponding peers that are owned by certain users specified by their e-mail address to access its resources and services.

With the PKI scheme described in this Recommendation, peers do not have to share passwords or secret information beforehand to implement these security mechanisms.

7 Information denoted in a peer device certificate

A peer device certificate has to contain the following information in order to make it verifiable.

– The e-mail address of the issuer:

  • The issuer field of the ITU-T X.509 certificate must contain the e-mail address of the issuer as the emailAddress attribute.

    e.g., issuer: CN=Alice/emailAddress=alice@example.com

– The uniform resource locator (URL) of the issuer's CA certificate:

  • The issuerAltName field of the ITU-T X.509 certificate must contain the URL of the issuer's CA certificate.

  • The URL of the issuer's CA certificate must take the form:

    https://usercert.<domain>:<port>/<username>.cer

    where <domain> is exactly the same as the domain part of the issuer's e-mail address (e.g., example.com), and <username> is the same as the local part of the e-mail address (e.g., alice). ":<port>" can be omitted.

    e.g., issuerAltName: https://usercert.example.com/alice.cer

– The URL of the CRL:

  • The cRLDistributionPoints field of the ITU-T X.509 certificate must contain the URL of the CRL.

  • The URL of the CRL must take the form:

    https://usercert.<domain>:<port>/<username>.crl

    where <domain> is exactly the same as the domain part of the issuer's e-mail address (e.g., example.com), and <username> is the same as the local part of the e-mail address (e.g., alice). ":<port>" can be omitted.

    e.g., cRLDistributionPoints: https://usercert.example.com/alice.crl

The correspondence between the e-mail address of the issuer and URLs for CA certificate and CRL must be obvious and HTTPS must be used in URLs.

In the above example, one can be sure that alice@example.com's CA certificate and CRL are published by alice@example.com's service provider (i.e., example.com), and not by another service provider such as example.net, and the integrity of those data is guaranteed by the HTTPS protocol used for retrieval. With this scheme, the CA certificate and CRL URLs for alice@example.com and alice@*subdomain*.example.com are different, and thus usercert.*subdomain*.example.com is only authorized to publish CA certificates and CRLs of <user>@*subdomain*.example.com. It cannot publish CA certificates and CRLs of <user>@example.com.

8 Operations provided by the service provider

8.1 Upload of CA certificate and CRL

A service provider has to provide its users an upload operation by which a user can authenticate herself/himself and upload and/or update her/his CA certificate and CRL.

8.2 Retrieval of CA certificate and CRL

A service provider has to make its users' CA certificate and CRL available for download by a URL which is constructed from the user's e-mail address and uses HTTPS as the protocol.

9 Peer entity authentication procedure

Peer entity authentication should follow the following procedures:

1) Receive a public key certificate from the corresponding peer.
2) Check the identity (e-mail address) of the issuer of the certificate and URLs for obtaining a CA certificate and CRL.
3) Verify the correspondence between the issuer's e-mail address and URLs for CA certificate and CRL. (The correct URLs assure the authenticity of the CA certificate and CRL.)
4) Retrieve the CA certificate and CRL. (The HTTPS protocol used for the retrieval guarantees the integrity of the CA certificate and CRL.)
5) Verify the authenticity and validity of the corresponding peer's certificate using the CA certificate and CRL downloaded in the previous step.
6) Perform a public key-based authentication protocol to verify that the corresponding peer possesses the private part of the key pair which is certified in its certificate.

10 Security considerations

10.1 Authenticity and integrity of CA certificates

Because the authenticity of a CA certificate is derived from its URL and its integrity is assured by the HTTPS protocol used for retrieval, peers should only trust freshly downloaded CA certificates. Local caches or copies may not be trusted.

10.2 Scope of peer devices' name

The distinguished name of the subject in a peer device certificate must not be interpreted in a global scope. For example, if a peer device owned by a user alice@example.com has a certificate whose subject field is "CN=www.example.com", it must not be interpreted as a valid fully qualified domain name (FQDN) of a server on the Internet. The scope of the name must be local to alice@example.com's perspective.

10.3 Trustworthiness of service providers

As service providers can forge their users' CA certificate, they can set up peer devices that impersonate a user's device. Therefore, service providers must be trustworthy. However, this issue is not specific to this PKI scheme. In the current Internet PKI, some well-known certification authorities issue S/MIME certificates to users after successful exchanges of a couple of e-mail messages, which enables a service provider to obtain a valid S/MIME certificate of any user of its e-mail service.

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1161] Recommendation ITU-T X.1161 (2008), *Framework for secure peer-to-peer communications*.

[b-ITU-T X.1162] Recommendation ITU-T X.1162 (2008), *Security architecture and operations for peer-to-peer networks*.

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	Terminals and subjective and objective assessment methods
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, 2013