

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1341

(09/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – PKI related
Recommendations

Certified mail transport and certified post office protocols

Recommendation ITU-T X.1341

ITU-T

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
PKI related Recommendations	X.1340–X.1349
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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1341

Certified mail transport and certified post office protocols

Summary

Recommendation ITU-T X.1341 defines the certified mail transfer protocol (CMTP) and certified post office protocol (CPOP) in order to foster exchange of electronic certified mails worldwide in a secure way by providing confidentiality, identification of the correspondents, integrity and non-repudiation.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1341	2015-09-17	17	11.1002/1000/12352

Keywords

Certified mail transfer protocol, certified post office protocol, CMTP, confidentiality, CPOP, integrity, non-repudiation, POP, post office protocol, security, simple mail transfer protocol, SMTP.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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 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 2016

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

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	2
4	Abbreviations and acronyms	3
5	Conventions	4
6	Certified mail basic concepts.....	4
7	Types of certified mail commands	4
	7.1 Types of CMTP commands.....	5
	7.2 Types of CPOP commands.....	5
8	Detailed CMTP specification	7
	8.1 CELO: Ask for delivery type list.....	7
	8.2 Delivery type list	7
	8.3 Selected delivery type.....	8
	8.4 Delivery type acknowledgement	8
	8.5 Sender's e-mail address.....	8
	8.6 Sender's e-mail acknowledgement	8
	8.7 Ask for sending e-mail to recipient	8
	8.8 Check recipient's e-mail address by the remote Cmail server	8
	8.9 Recipient's e-mail address acknowledgement	9
	8.10 Recipient's e-mail acknowledgement	9
	8.11 Ask for sending ENVELOPE	9
	8.12 Ready to receive ENVELOPE.....	10
	8.13 ENVELOPE	10
	8.14 Server signed notice of deposit.....	10
	8.15 Sender and server signed notice of deposit	10
	8.16 ENVELOPE between Cmail servers	11
	8.17 Signed notice of transit between Cmail servers	11
	8.18 Signed notice of transit.....	11
9	Certified post office protocol (CPop)	12
	9.1 Ask for pending messages	12
	9.2 Challenge recipient and server signed notice of reception.....	12
	9.3 Challenge response and recipient and server signed notice of reception	13
	9.4 ENVELOPE	14
	9.5 Recipient and server signed notice of reception between Cmail servers (optional)	14
	9.6 Recipient and server signed notice of reception.....	14
Annex A	– Notices in XML schema definition (XSD).....	15
	A.1 XSD overview	15



Documents

Document Sharing Hub

Rec. ITU-T X.1341 (09/2015)

iii

	Page
A.2 Formal specification of notices in XSD	18
Annex B – Notices in ASN.1	22
Annex C – Requirements on public-key infrastructure components	26
C.1 Introduction	26
C.2 Cmail server end-entity public-key certificates.....	26
C.3 Cmail client end-entity public-key certificates.....	26
C.4 Information validation requirements	27
Annex D – Requirements on transport layer security (TLS)	28
Annex E – Object identifiers defined in this Recommendation.....	29
Appendix I – Envelope and notices format.....	30
I.1 Notice of deposit.....	30
I.2 Notice of reception	30
I.3 Notice of transit	31
I.4 ENVELOPE	32
Bibliography.....	33

Introduction

This Recommendation extends the capabilities of the simple mail transfer protocol (SMTP) and post office protocol version 3 (POP3) to support authentication, security and non-repudiation.

For this purpose, two protocols are specified:

- the certified mail transfer protocol (CMTP), which is an extension to the simple mail transfer protocol (SMTP), is the protocol supporting the communications between the sender of e-mails and a mail server, called the certified mail (Cmail) server;
- the certified post office protocol (CPOP), which is an extension to the post office protocol version 3 (POP3), is the protocol supporting the communications between the recipient of e-mails and the Cmail server.

Within SMTP and POP3, a message type is identified by a command, i.e., a keyword at the start of the message. For CMTP and CPOP, new commands have been defined and some of the SMTP and POP3 commands have been extended. In particular, some commands have been extended to carry notices (electronic documents) allowing the different stages of the communication from the sender to the recipient to be documented and verified.

CMTP and CPOP also introduce the concept of Cmail server that is an active partner in the communication between the sender and the recipient allowing it to certify that the exchange between two parties has indeed occurred.

Certified mail assumes that an existing public-key infrastructure (PKI) is established.

Annex A, which is an integral part of this Recommendation, provides the formal specification for notices using the XML schema definition (XSD) notation technique.

Annex B, which is an integral part of this Recommendation, provides the formal specification for notices using the abstract syntax notation one (ASN.1).

Annex C, which is an integral part of this Recommendation, specifies the requirements for public-key certificates issued to clients (sender and recipient of e-mails) and Cmail servers.

Annex D, which is an integral part of this Recommendation, specifies requirements on the use of the transport layer security (TLS) specification.

Annex E, which is an integral part of this Recommendation, specifies object identifiers defined for Cmail servers.

Recommendation ITU-T X.1341

Certified mail transport and certified post office protocols

1 Scope

This Recommendation specifies how to make e-mails reliable in terms of identification and confidentiality.

Certified mail transfer protocol/certified post office protocol (CMTP/CPOP) enables:

- the solution of repudiation issues because of the use of electronic signature;
- the solution of confidentiality issues because of the use of encryption;
- the production of reliable notices of deposit, notices of transit and notices of reception;
- the use of a certified mail (Cmail) server to track certified mails to avoid their loss during the process;
- the use of a transport layer security (TLS) connection to provide stronger identification. This stronger level of identification is required by the Cmail server.

Conformity with this Recommendation is not to be taken as any proof of evidence for claiming compliance with any national or regional law, regulation or policy. The technical, organizational and procedural means described in this Recommendation do not guarantee in any way the constitution of any level of security that may be put upon certain correspondence by specific national or regional law, regulation or policy.

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.520](#)] Recommendation ITU-T X.520 (2012) | ISO/IEC 9594-6:2014, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- [[ITU-T X.680](#)] Recommendation ITU-T X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- [[ITU-T X.690](#)] Recommendation ITU-T X.690 (2008) | ISO/IEC 8825-1: 2008, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
- [[ITU-T X.693](#)] Recommendation ITU-T X.693 (2008) | ISO/IEC 8825-4: 2008, *Information technology – ASN.1 encoding rules: XML Encoding Rules (XER)*.
- [ISO 3166-1] ISO 3166-1:2013, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes*.

[IETF RFC 822]	IETF RFC 822 (1982), <i>Standard for the format of ARPA Internet text messages</i> .
[IETF RFC 1939]	IETF RFC 1939 (1996), <i>Post office protocol – Version 3</i> .
[IETF RFC 2045]	IETF RFC 2045 (1996), <i>Multipurpose internet mail extensions (MIME) – Part One: Format of internet message bodies</i> .
[IETF RFC 5246]	IETF RFC 5246 (2008), <i>The transport layer security (TLS) Protocol – Version 1.2</i> .
[IETF RFC 5321]	IETF RFC 5321 (2008), <i>Simple mail transfer protocol</i> .
[XML]	W3C Recommendation XML1.0 (2000), <i>Extensible markup language (XML) 1.0 (fifth edition)</i> .
[XSD]	W3C Recommendation XML Schema (2001), <i>XML schema Part 1: Structures</i> .

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 certification authority (CA) [[b-ITU-T X.509](#)]: An authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority may create the subjects' keys.

3.1.2 certificate validation [[b-ITU-T X.509](#)]: The process of ensuring that a certificate was valid at a given time, including possibly the construction and processing of a certification path, and ensuring that all certificates in that path were valid (i.e., were not expired or revoked) at that given time.

3.1.3 hash function [[b-ITU-T X.509](#)]: A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range.

3.1.4 private key [[b-ITU-T X.509](#)]: (In a public key cryptosystem) that key of an entity's key pair which is known only by that entity.

3.1.5 public key [[b-ITU-T X.509](#)]: (In a public key cryptosystem) that key of a user's key pair which is publicly known.

3.1.6 public-key certificate (PKC) [[b-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 CA which issued it.

3.1.7 public-key infrastructure (PKI) [[b-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

This Recommendation defines the following terms:

3.2.1 certified mail: Electronic mail exchanged using the certified mail transfer protocol (CMTP) and certified post office protocol (CPOP).

3.2.2 certified mail transfer protocol (CMTP): Application layer protocol over the transmission control protocol/Internet protocol (TCP/IP) connection based on the simple mail transfer protocol (SMTP) used to send certified mail.

3.2.3 certified post office protocol (CPOP): Application layer protocol over the transmission control protocol/Internet protocol (TCP/IP) connection based on the post office protocol version 3 (POP3) used to receive certified mail.

3.2.4 Cmail server: Trusted entity involved in certified mail transactions.

3.2.5 notice of deposit: Electronic document signed by the sender and the Cmail server, containing information allowing the occurrence of a certified mail deposit to be certified.

3.2.6 notice of reception: Electronic document signed by the recipient and the Cmail server, containing information allowing the reception by the recipient of a certified mail to be certified.

3.2.7 notice of transit: Electronic document signed by the Cmail servers involved in the transaction and containing information allowing the transmission to the Cmail server of a certified mail to be certified.

3.2.8 post office protocol version 3 (POP3): Application layer protocol over the transmission control protocol/Internet protocol (TCP/IP) connection used to receive e-mail.

3.2.9 simple mail transfer protocol (SMTP): Application layer protocol over the transmission control protocol/Internet protocol (TCP/IP) connection used to send e-mail.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AES	Advanced Encryption Standard
ASN.1	Abstract Syntax Notation One
CA	Certification Authority
CBC	Cipher Block Chaining
Cmail	Certified Mail
CMTP	Certified Mail Transfer Protocol
CPOP	Certified Post Office Protocol
DER	Distinguished Encoding Rules
DNS	Domain Name System
id	identity
MIME	Multipurpose Internet Mail Extensions
PKI	Public-Key Infrastructure
POP3	Post Office Protocol version 3
RSA	Rivest, Shamir and Adleman algorithm
RSCK	Random Symmetric Cipher Key
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

TLS	Transport Layer Security
UTF-8	Universal Character Set Transformation Format-8
XER	XML Encoding Rules
XML	eXtensible Markup Language
XSD	XML Schema Definition

5 Conventions

None.

6 Certified mail basic concepts

In traditional e-mail communications using the simple mail transfer protocol (SMTP) and post office protocol version 3 (POP3) a recipient of an e-mail can deny ever having received it. This is even the case when secure/multipurpose internet mail extensions (S/MIME) is added to the protocol suite. S/MIME provides for encryption of messages and authentication of the sender, but it does not provide proof of delivery.

This Recommendation specifies a protocol suite called certified mail that comprises the certified mail transfer protocol (CMTP) and the certified post office protocol (CPOP).

In SMTP/POP3 communications, the mail server is not an active part in the communications, but is only forwarding messages as they are received when the recipient signs on to the mail server. This is even the case when S/MIME is employed.

In certified mail, the mail server actively participates in the communication between the sender and the recipient in a way that allows the Cmail server to verify that the recipient has accepted to receive the mail. The mail is sent encrypted, not allowing the Cmail server to read the actual content of the e-mail. An overview of the procedure is given in the following, while a detailed specification is given in clause 8.

The interactions between the sender and the Cmail server are specified in clause 8.

The interactions between the recipient and the Cmail server are specified in clause 9.

7 Types of certified mail commands

Certified mail makes use of a combination of current SMTP and POP3 commands, some enhanced SMTP and POP3 commands and some certified mail specific commands. In Tables 1 and 2, commands that do not have a counterpart in SMTP/POP3 are labelled "Additional". Commands that are enhanced SMTP/POP3 commands are labelled "Modified". SMTP/POP3 commands that are used unchanged are labelled "Unchanged".

A command type is defined as a keyword using upper case letters that identifies a particular message type together with some additional specifications for that message type.

7.1 Types of CMTP commands

Table 1 – CMTP commands

Command	Command function
CELO Additional	Enables the server to identify its processing of CMTP commands.
DELV Additional	Identifies the delivery mode: certifiedMail.
MAIL FROM Modified	Identifies the sender of the message; used as "MAIL FROM". If the account exists on the server, then it sends back a base64 of the public-key certificate of the known sender.
RCPT TO Modified	Identifies the recipients of the message; used under "RCPT TO" format. If the account exists on the server, then it sends back a base64 of the public-key certificate of the known sender. If the account exists on another CMTP server with which key exchanges have been made, then the server questions the second server and sends a base64 of the public-key certificate belonging to the known recipient with the CHCK RCPT command.
CHCK RCPT Additional	Sent only if the recipient is attached to another Cmail server than the Cmail server for the sender.
DATA Modified	Sent by a client to initiate the transfer of message content. The server sends back in a notice of deposit signed by the server and to be signed by the sender.
DEPO Additional	Sent by a client to initiate the transfer of the notice of deposit content signed by the server and countersigned by the sender.
SEND EVLP Additional	Forwards envelope from one Cmail server to another.
HELP Unchanged	Returns a list of commands that are supported by the CMTP server.
QUIT Unchanged	Terminates the session.

7.2 Types of CPOP commands

Table 2 – CPOP commands

Command	Command function
USER Unchanged	Used to specify the name of the user who is logging on.
PASS Unchanged	Password of the user who is logging on.
LIST Modified	Used to list messages and their combined size. For example, invoking the LIST command with no parameters will return 2 +OK messages (320 octets), and the list of messages: identity (id), length and delivery mode (if any) like CertifiedMail.

Table 2 – CPOP commands

Command	Command function
RETR Modified	Where N is a number between 1 and the last number returned by the LIST command. This command may not be used to retrieve a message that has been marked as deleted. If there is no delivery type, the server sends the e-mail in multipurpose Internet mail extensions (MIME) encoding. If delivery mode is defined, the server processes the message specifically. For example with CertifiedMail, the server challenges the recipient before sending the envelope by using RCPT command.
CHLG RESP Additional	Sent by the client to give notice of reception for the message and give the reply to the secret question. If the reply is correct then the server sends back the MIME envelope.
SEND NORP Additional	Sends the signed notice of reception.
HELP Unchanged	Returns a list of command that is supported by the CPOP server.
QUIT Unchanged	Terminates the session.