

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.500

(10/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Directory

**Information technology – Open Systems
Interconnection –The Directory: Overview
of concepts, models and services**

Recommendation ITU-T X.500

ITU-T

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

INFORMATION AND NETWORK SECURITY

X.1000–X.1099

SECURE APPLICATIONS AND SERVICES

X.1100–X.1199

CYBERSPACE SECURITY

X.1200–X.1299

SECURE APPLICATIONS AND SERVICES

X.1300–X.1399

CYBERSECURITY INFORMATION EXCHANGE

X.1500–X.1599

CLOUD COMPUTING SECURITY

X.1600–X.1699

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

**INTERNATIONAL STANDARD ISO/IEC 9594-1
RECOMMENDATION ITU-T X.500**

**Information technology – Open Systems Interconnection – The Directory: Overview of
concepts, models and services**

Summary

Recommendation ITU-T X.500 | International Standard ISO/IEC 9594-1 introduces the concepts of the Directory and the DIB (Directory Information Base) and overviews the services and capabilities which they provide.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.500	1988-11-25		11.1002/1000/2995
2.0	ITU-T X.500	1993-11-16	7	11.1002/1000/2996
3.0	ITU-T X.500	1997-08-09	7	11.1002/1000/4121
3.1	ITU-T X.500 (1997) Amd. 1	2000-03-31	7	11.1002/1000/5029
4.0	ITU-T X.500	2001-02-02	7	11.1002/1000/5307
5.0	ITU-T X.500	2005-08-29	17	11.1002/1000/8488
6.0	ITU-T X.500	2008-11-13	17	11.1002/1000/9587
7.0	ITU-T X.500	2012-10-14	17	11.1002/1000/11732
8.0	ITU-T X.500	2016-10-14	17	11.1002/1000/13029

Keywords

Attribute, directory, directory information tree, directory system agent, directory user agent, distinguished name.

* 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 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 2016

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

CONTENTS

	<i>Page</i>
1 Scope	1
2 Normative references.....	1
2.1 Identical Recommendations International Standards	1
3 Definitions	2
3.1 Communication model definitions	2
3.2 Directory model definitions	2
3.3 Distributed Operation definitions	3
3.4 Replication definitions	3
3.5 Basic directory definitions	3
4 Abbreviations	3
5 Conventions.....	3
6 Overview of the Directory	4
7 The Directory Information Base (DIB)	5
8 The Directory service	7
8.1 Introduction	7
8.2 Service qualification.....	7
8.3 Directory interrogation.....	8
8.4 Directory modification	8
8.5 Other outcomes	9
9 The distributed Directory	9
9.1 Functional model.....	9
9.2 Organizational model	9
9.3 Operation of the model.....	10
10 Access control in the Directory	13
11 Service administration	14
12 Replication in the Directory	14
12.1 Introduction	14
12.2 Forms of Directory replication	15
12.3 Replication and consistency of Directory information.....	16
12.4 Views of replication	16
12.5 Replication and Access Control	17
13 Directory protocols.....	17
14 Systems management of the Directory	17
14.1 Introduction	17
14.2 Management of the DIT domain	17
14.3 Management of Directory components	18
Annex A – Applying the Directory.....	19
A.1 The Directory environment	19
A.2 Directory service characteristics	19
A.3 Patterns of use of the Directory	19
Annex B – Amendments and corrigenda	23

Introduction

This Recommendation | International Standard together with other Recommendations | International Standards, has been produced to facilitate the interconnection of information processing systems to provide directory services. A set of such systems, together with the directory information that they hold, can be viewed as an integrated whole, called the *Directory*. The information held by the Directory, collectively known as the Directory Information Base (DIB), is typically used to facilitate communication between, with or about objects such as application entities, people, terminals and distribution lists.

The Directory plays a significant role in Open Systems Interconnection, whose aim is to allow, with a minimum of technical agreement outside of the interconnection standards themselves, the interconnection of information processing systems:

- from different manufacturers;
- under different managements;
- of different levels of complexity; and
- of different ages.

This Recommendation | International Standard introduces and models the concepts of the Directory and of the DIB and overviews the services and capabilities which they provide. Other Recommendations | International Standards make use of these models in defining the abstract service provided by the Directory, and in specifying the protocols through which this service can be obtained or propagated.

This Recommendation | International Standard provides the foundation frameworks upon which industry profiles can be defined by other standards groups and industry forums. Many of the features defined as optional in these frameworks, may be mandated for use in certain environments through profiles. This eighth edition technically revises and enhances, the seventh edition of this Recommendation | International Standard.

This eighth edition specifies versions 1 and 2 of the Directory protocols.

The first and second editions specified only version 1. Most of the services and protocols specified in this edition are designed to function under version 1. However some enhanced services and protocols, e.g., signed errors, will not function unless all Directory entities involved in the operation have negotiated version 2. Whichever version has been negotiated, differences between the services and between the protocols defined in the seven editions, except for those specifically assigned to version 2, are accommodated using the rules of extensibility defined in Rec. ITU-T X.519 | ISO/IEC 9594-5.

Annex A, which is an integral part of this Recommendation | International Standard, describes the types of use to which the Directory can be applied.

Annex B, which is not an integral part of this Recommendation | International Standard, lists the amendments and defect reports that have been incorporated to form this edition of this Recommendation | International Standard.

iv

**INTERNATIONAL STANDARD
ITU-T RECOMMENDATION**

Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services

1 Scope

The Directory provides the directory capabilities required by OSI applications, OSI management processes, other OSI layer entities, and telecommunications services. Among the capabilities which it provides are those of "user-friendly naming", whereby objects can be referred to by names which are suitable for citing by human users (though not all objects need have user-friendly names); and "name-to-address mapping" which allows the binding between objects and their locations to be dynamic. The latter capability allows OSI networks, for example, to be "self-configuring" in the sense that addition, removal and the changes of object location do not affect OSI network operation.

The Directory is not intended to be a general-purpose database system, although it may be built on such systems. It is assumed, for instance, that, as is typical with communications directories, there is a considerably higher frequency of "queries" than of updates. The rate of updates is expected to be governed by the dynamics of people and organizations, rather than, for example, the dynamics of networks. There is also no need for instantaneous global commitment of updates; transient conditions, where both old and new versions of the same information are available, are quite acceptable.

It is a characteristic of the Directory that, except as a consequence of differing access rights or un-propagated updates, the results of directory queries will not be dependent on the identity or location of the inquirer. This characteristic renders the Directory unsuitable for some telecommunications applications, for example some types of routing. For cases where the results are dependent on the identity of the inquirer, access to directory information and updates of the Directory may be denied.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The basic model.*
- Recommendation ITU-T X.501 (2016) | ISO/IEC 9594-2:2017, *Information technology – Open Systems Interconnection – The Directory: Models.*
- Recommendation ITU-T X.509 (2016) | ISO/IEC 9594-8:2017, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*
- Recommendation ITU-T X.511 (2016) | ISO/IEC 9594-3:2017, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition.*
- Recommendation ITU-T X.518 (2016) | ISO/IEC 9594-4:2017, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation.*
- Recommendation ITU-T X.519 (2016) | ISO/IEC 9594-5:2017, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications.*
- Recommendation ITU-T X.520 (2016) | ISO/IEC 9594-6:2017, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types.*
- Recommendation ITU-T X.521 (2016) | ISO/IEC 9594-7:2017, *Information technology – Open Systems Interconnection – The Directory: Selected object classes.*
- Recommendation ITU-T X.525 (2016) | ISO/IEC 9594-9:2017, *Information technology – Open Systems Interconnection – The Directory: Replication.*

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 Communication model definitions

The following terms are defined in Rec. ITU-T X.519 | ISO/IEC 9594-5:

- a) application-entity;
- b) application layer;
- c) application process.

3.2 Directory model definitions

The following terms are defined in Rec. ITU-T X.501 | ISO/IEC 9594-2:

- a) access control;
- b) Administration Directory Management Domain;
- c) alias;
- d) ancestor;
- e) attribute;
- f) attribute type;
- g) attribute value;
- h) authentication;
- i) compound entry;
- j) context;
- k) Directory Information Tree (DIT);
- l) Directory Management Domain (DMD);
- m) Directory System Agent (DSA);
- n) Directory User Agent (DUA);
- o) distinguished name;
- p) entry;
- q) family (of entries);
- r) hierarchical group;
- s) LDAP client;
- t) LDAP requester;
- u) LDAP responder;
- v) LDAP server;
- w) name;
- x) object (of interest);
- y) Private Directory Management Domain;
- z) related entries;
- aa) relative distinguished name;
- bb) root;
- cc) schema;
- dd) security policy;
- ee) subordinate object;
- ff) superior entry;
- gg) superior object;
- hh) tree.

3.3 Distributed Operation definitions

The following terms are defined in Rec. ITU-T X.518 | ISO/IEC 9594-4:

- a) uni-chaining;
- b) multi-chaining;
- c) referral.

3.4 Replication definitions

The following terms are defined in Rec. ITU-T X.525 | ISO/IEC 9594-9:

- a) caching;
- b) cache copy;
- c) entry copy;
- d) master DSA;
- e) replication;
- f) shadow consumer;
- g) shadow supplier;
- h) shadowed information;
- i) shadowing agreement.

3.5 Basic directory definitions

The following terms are defined in this Recommendation | International Standard:

3.5.1 the Directory: A collection of open systems cooperating to provide directory services.

3.5.2 directory information base (DIB): The set of information managed by the Directory.

3.5.3 (directory) user: The end user of the Directory, i.e., the entity or person which accesses the Directory.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ACI	Access Control Information
DAP	Directory Access Protocol
DIB	Directory Information Base
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DMD	Directory Management Domain
DOP	Directory Operational Binding Management Protocol
DSA	Directory System Agent
DSP	Directory System Protocol
DUA	Directory User Agent
LDAP	Lightweight Directory Access Protocol
OSI	Open Systems Interconnection
RDN	Relative Distinguished Name

5 Conventions

With minor exceptions this Directory Specification has been prepared according to the November 2001 edition of the *Rules for presentation of ITU-T | ISO/IEC common text*.

The term "Directory Specification" (as in "this Directory Specification") shall be taken to mean Rec. ITU-T X.500 | ISO/IEC 9594-1. The term "Directory Specifications" shall be taken to mean the ITU-T X.500-series Recommendations, except for Rec. ITU-T X.509, and all parts of ISO/IEC 9594, except for ISO/IEC 9594-8.

This Directory Specification uses the term *first edition systems* to refer to systems conforming to the first edition of these Directory Specifications, i.e., the 1988 edition of the series of CCITT X.500 Recommendations and the ISO/IEC 9594:1990 edition.

This Directory Specification uses the term *second edition systems* to refer to systems conforming to the second edition of these Directory Specifications, i.e., the 1993 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:1995 edition.

This Directory Specification uses the term *third edition systems* to refer to systems conforming to the third edition of these Directory Specifications, i.e., the 1997 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:1998 edition.

This Directory Specification uses the term *fourth edition systems* to refer to systems conforming to the fourth edition of the Directory Specifications, i.e., the 2001 editions of Recs ITU-T X.500, ITU-T X.501, ITU-T X.511, ITU-T X.518, ITU-T X.519, ITU-T X.520, ITU-T X.521, ITU-T X.525, and ITU-T X.530, the 2000 edition of Rec. ITU-T X.509, and parts 1-10 of the ISO/IEC 9594:2001 edition.

This Directory Specification uses the term *fifth edition systems* to refer to systems conforming to the fifth edition of these Directory Specifications, i.e., the 2005 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:2005 edition.

This Directory Specification uses the term *sixth edition systems* to refer to systems conforming to the sixth edition of these Directory Specifications, i.e., the 2008 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:2008 edition.

This Directory Specification uses the term *seventh edition systems* to refer to systems conforming to the seventh edition of these Directory Specifications, i.e., the 2012 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:2014 edition.

This Directory Specification uses the term *eighth edition systems* to refer to systems conforming to the eighth edition of these Directory Specifications, i.e., the 2016 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:2016 edition.

This Directory Specification presents ASN.1 notation in the **bold Courier New** typeface. When ASN.1 types and values are referenced in normal text, they are differentiated from normal text by presenting them in the **bold Courier New** typeface. The names of procedures, typically referenced when specifying the semantics of processing, are differentiated from normal text by displaying them in **bold Times New Roman**. Access control permissions are presented in *italicized Times New Roman*.

6 Overview of the Directory

The *Directory* is a collection of open systems which cooperate to hold a logical database of information about a set of objects in the real world. The *users* of the Directory, including people and computer programs, can read or modify the information, or parts of it, subject to having permission to do so. Each user is represented in accessing the Directory by a Directory User Agent (DUA) or an LDAP client, each of which is considered to be an application-process. These concepts are illustrated in Figure 1.

NOTE – The Directory Specifications refer to the Directory in the singular, and reflects the intention to create, through a single, unified, name space, one logical directory composed of many systems and serving many applications. Whether or not these systems choose to interwork will depend on the needs of the applications they support. Applications dealing with non-intersecting worlds of objects may have no such need. The single name space facilitates later interworking should the needs change. For a variety of reasons, such as security, connectivity, or business decisions, it is likely that some portions of the Directory may be unreachable from other portions of the Directory using third edition operations. This results in differing views of the Directory. Such differing views may contain related entries about a given real world object. Such related entries may or may not have the same distinguished name. Using fourth or subsequent edition systems, it is possible to perform operations across multiple, differing views to provide an integrated response to the user. Specifically:

- DMD administrators (see 9.2) may have a need to publish their own view (or views) of some specific real-world object; a real-world object may thus be modelled by multiple independent entries in the directory. This may happen whether or not they need to interwork. Interworking using DSP may also be unsupported.
- Notwithstanding the last sentence of the Note, it is also possible that particular DMDs may choose to publish information about real-world objects within their own distinct directory name-spaces (i.e., in one of multiple DITs); in this case, it would be possible to have a specific real-world object modelled by entries in the same or different DIT namespaces, with the same or different distinguished names in each. Note that certain Directory facilities (e.g., the acquisition of certificates, and related