
**Information technology — Open Systems
Interconnection — The Directory: Models**

*Technologies de l'information — Interconnexion de systèmes ouverts
(OSI) — L'annuaire: Les modèles*

Withdrawn

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Withdrawn



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published by ISO in 2009

Published in Switzerland

CONTENTS

	<i>Page</i>
Foreword	viii
Introduction	ix
SECTION 1 – GENERAL	1
1 Scope	1
2 Normative references	2
2.1 Identical Recommendations International Standards	2
2.2 Paired Recommendations International Standards equivalent in technical content.....	2
2.3 Other references.....	3
3 Definitions	3
3.1 Communication definitions	3
3.2 Basic Directory definitions.....	3
3.3 Distributed operation definitions	3
3.4 Replication definitions	3
4 Abbreviations	4
5 Conventions	4
SECTION 2 – OVERVIEW OF THE DIRECTORY MODELS	6
6 Directory Models.....	6
6.1 Definitions.....	6
6.2 The Directory and its users.....	6
6.3 Directory and DSA Information Models	7
6.4 Directory Administrative Authority Model.....	8
SECTION 3 – MODEL OF DIRECTORY USER INFORMATION	9
7 Directory Information Base	9
7.1 Definitions.....	9
7.2 Objects.....	10
7.3 Directory entries	10
7.4 Directory Information Tree (DIT).....	10
8 Directory entries.....	11
8.1 Definitions.....	11
8.2 Overall structure.....	13
8.3 Object classes.....	14
8.4 Attribute Types.....	16
8.5 Attribute Values.....	16
8.6 Attribute Type Hierarchies.....	16
8.7 Friend attributes.....	17
8.8 Contexts.....	17
8.9 Matching rules.....	18
8.10 Entry collections	21
8.11 Compound entries and families of entries.....	22
9 Names.....	23
9.1 Definitions.....	23
9.2 Names in general	23
9.3 Relative Distinguished Names	23
9.4 Name matching.....	25
9.5 Names returned during operations	25
9.6 Names held as attribute values or used as parameters	25
9.7 Distinguished Names	26
9.8 Alias Names.....	27
10 Hierarchical groups.....	27
10.1 Definitions.....	27
10.2 Hierarchical relationship.....	28
10.3 Sequential ordering of a hierarchical group	28

	<i>Page</i>
SECTION 4 – DIRECTORY ADMINISTRATIVE MODEL.....	30
11 Directory Administrative Authority model.....	30
11.1 Definitions.....	30
11.2 Overview.....	30
11.3 Policy	31
11.4 Specific administrative authorities	31
11.5 Administrative areas and administrative points	32
11.6 DIT Domain policies	34
11.7 DMD policies.....	34
SECTION 5 – MODEL OF DIRECTORY ADMINISTRATIVE AND OPERATIONAL INFORMATION	36
12 Model of Directory Administrative and Operational Information	36
12.1 Definitions.....	36
12.2 Overview.....	36
12.3 Subtrees	37
12.4 Operational attributes.....	39
12.5 Entries	40
12.6 Subentries.....	40
12.7 Information model for collective attributes	41
12.8 Information model for context defaults.....	42
SECTION 6 – THE DIRECTORY SCHEMA.....	43
13 Directory Schema	43
13.1 Definitions.....	43
13.2 Overview.....	43
13.3 Object class definition.....	45
13.4 Attribute type definition	46
13.5 Matching rule definition	49
13.6 Relaxations and tightenings.....	51
13.7 DIT structure definition.....	57
13.8 DIT content rule definition.....	59
13.9 Context type definition.....	61
13.10 DIT Context Use definition.....	62
13.11 Friends definition.....	63
14 Directory System Schema	63
14.1 Overview.....	63
14.2 System schema supporting the administrative and operational information model	64
14.3 System schema supporting the administrative model	64
14.4 System schema supporting general administrative and operational requirements.....	65
14.5 System schema supporting access control	67
14.6 System schema supporting the collective attribute model	67
14.7 System schema supporting context assertion defaults	68
14.8 System schema supporting the service administration model.....	68
14.9 System schema supporting hierarchical groups.....	68
14.10 Maintenance of system schema	69
14.11 System schema for first-level subordinates	70
15 Directory schema administration	70
15.1 Overview.....	70
15.2 Policy objects.....	70
15.3 Policy parameters.....	70
15.4 Policy procedures.....	71
15.5 Subschema modification procedures	71
15.6 Entry addition and modification procedures.....	72
15.7 Subschema policy attributes	72

	<i>Page</i>
SECTION 7 – DIRECTORY SERVICE ADMINISTRATION	78
16 Service Administration Model.....	78
16.1 Definitions.....	78
16.2 Service-type/user-class model.....	78
16.3 Service-specific administrative areas.....	79
16.4 Introduction to search-rules.....	80
16.5 Subfilters.....	80
16.6 Filter requirements	81
16.7 Attribute information selection based on search-rules	81
16.8 Access control aspects of search-rules	81
16.9 Contexts aspects of search-rules.....	82
16.10 Search-rule specification	82
16.11 Matching restriction definition.....	90
16.12 Search-validation function	90
SECTION 8 – SECURITY	91
17 Security model.....	91
17.1 Definitions.....	91
17.2 Security policies	91
17.3 Protection of Directory operations	92
18 Basic Access Control	93
18.1 Scope and application	93
18.2 Basic Access Control model.....	93
18.3 Access control administrative areas	95
18.4 Representation of Access Control Information	98
18.5 ACI operational attributes.....	103
18.6 Protecting the ACI.....	104
18.7 Access control and Directory operations	104
18.8 Access Control Decision Function.....	104
18.9 Simplified Access Control	106
19 Rule-based Access Control.....	106
19.1 Scope and application	106
19.2 Rule-based Access Control model	107
19.3 Access control administrative areas	107
19.4 Security Label	107
19.5 Clearance	109
19.6 Access Control and Directory operations	109
19.7 Access Control Decision Function.....	110
19.8 Use of Rule-based and Basic Access Control.....	110
20 Data Integrity in Storage	110
20.1 Introduction	110
20.2 Protection of an Entry or Selected Attribute Types.....	110
20.3 Context for Protection of a Single Attribute Value.....	112
SECTION 9 – DSA MODELS.....	113
21 DSA Models.....	113
21.1 Definitions.....	113
21.2 Directory Functional Model	113
21.3 Directory Distribution Model	114

	<i>Page</i>
SECTION 10 – DSA INFORMATION MODEL.....	116
22 Knowledge.....	116
22.1 Definitions.....	116
22.2 Introduction	116
22.3 Knowledge References.....	117
22.4 Minimum Knowledge	119
22.5 First Level DSAs	120
23 Basic Elements of the DSA Information Model	120
23.1 Definitions.....	120
23.2 Introduction	120
23.3 DSA Specific Entries and their Names	121
23.4 Basic Elements	122
24 Representation of DSA Information	124
24.1 Representation of Directory User and Operational Information	124
24.2 Representation of Knowledge References	125
24.3 Representation of Names and Naming Contexts	131
SECTION 11 – DSA OPERATIONAL FRAMEWORK.....	133
25 Overview	133
25.1 Definitions.....	133
25.2 Introduction	133
26 Operational bindings	133
26.1 General	133
26.2 Application of the operational framework.....	134
26.3 States of cooperation.....	135
27 Operational binding specification and management.....	136
27.1 Operational binding type specification.....	136
27.2 Operational binding management	137
27.3 Operational binding specification templates	137
28 Operations for operational binding management.....	139
28.1 Application-context definition	139
28.2 Establish Operational Binding operation.....	140
28.3 Modify Operational Binding operation	142
28.4 Terminate Operational Binding operation	143
28.5 Operational Binding Error.....	144
28.6 Operational Binding Management Bind and Unbind	145
Annex A – Object identifier usage.....	146
Annex B – Information Framework in ASN.1.....	149
Annex C – SubSchema Administration Schema in ASN.1.....	159
Annex D – Service Administration in ASN.1.....	163
Annex E – Basic Access Control in ASN.1	167
Annex F – DSA Operational Attribute Types in ASN.1	171
Annex G – Operational Binding Management in ASN.1	174
Annex H – Enhanced security.....	178
Annex I – The Mathematics of Trees	181
Annex J – Name Design Criteria	182

	<i>Page</i>
Annex K – Examples of various aspects of schema	184
K.1 Example of an attribute hierarchy	184
K.2 Example of a subtree specification	184
K.3 Schema specification	185
K.4 DIT content rules	186
K.5 DIT context use	187
Annex L – Overview of basic access control permissions	188
L.1 Introduction	188
L.2 Permissions required for operations	188
L.3 Permissions affecting error	189
L.4 Entry level permissions	189
L.5 Entry level permissions	190
Annex M – Examples of access control	192
M.1 Introduction	192
M.2 Design principles for Basic Access Control	192
M.3 Introduction to example	192
M.4 Policy affecting the definition of specific and inner areas	193
M.5 Policy affecting the definition of DACDs	195
M.6 Policy expressed in prescriptive ACI attributes	197
M.7 Policy expressed in subentry ACI attributes	202
M.8 Policy expressed in entry ACI attributes	203
M.9 ACDF examples	204
M.10 Rule-based Access Control	206
Annex N – DSE type combinations	207
Annex O – Modelling of knowledge	209
Annex P – Names held as attribute values or used as parameters	214
Annex Q – Subfilters	215
Annex R – Compound entry name patterns and their use	216
Annex S – Naming concepts and considerations	218
S.1 History tells us	218
S.2 A new look at name resolution	218
Annex T – Alphabetical index of definitions	224
Annex U – Amendments and corrigenda	226

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 9594-2:2008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.501 (11/2008).

This sixth edition cancels and replaces the fifth edition (ISO/IEC 9594-2:2005), which has been technically revised.

ISO/IEC 9594 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — The Directory*:

- *Part 1: Overview of concepts, models and services*
- *Part 2: Models*
- *Part 3: Abstract service definition*
- *Part 4: Procedures for distributed operation*
- *Part 5: Protocol specifications*
- *Part 6: Selected attribute types*
- *Part 7: Selected object classes*
- *Part 8: Public-key and attribute certificate frameworks*
- *Part 9: Replication*
- *Part 10: Use of systems management for administration of the Directory*

Introduction

This Recommendation | International Standard, together with the 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 provides a number of different models for the Directory as a framework for the other Recommendations in the ITU-T X.500 series | parts of ISO/IEC 9594. The models are the overall (functional) model; the administrative authority model, generic Directory Information Models providing Directory User and Administrative User views on Directory information, generic DSA and DSA information models, an Operational Framework and a security model.

The generic Directory Information Models describe, for example, how information about objects is grouped to form Directory entries for those objects and how that information provides names for objects.

The generic DSA and DSA information models and the Operational Framework provide support for Directory distribution.

This Recommendation | International Standard provides a specialization of the generic Directory Information Models to support Directory Schema administration.

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 sixth edition technically revises and enhances, but does not replace, the fifth edition of this Recommendation | International Standard. Implementations may still claim conformance to the fifth edition. However, at some point, the fifth edition will not be supported (i.e., reported defects will no longer be resolved). It is recommended that implementations conform to this sixth edition as soon as possible.

This sixth 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 six editions, except for those specifically assigned to version 2, are accommodated using the rules of extensibility defined in ITU-T Rec. X.519 | ISO/IEC 9594-5.

Annex A, which is an integral part of this Recommendation | International Standard, summarizes the usage of ASN.1 object identifiers in the ITU-T X.500-series Recommendations | parts of ISO/IEC 9594.

Annex B, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module which contains all of the definitions associated with the information framework.

Annex C, which is an integral part of this Recommendation | International Standard, provides the subschema administration schema in ASN.1.

Annex D, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for Service Administration.

Annex E, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module for Basic Access Control.

Annex F, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module which contains all the definitions associated with DSA operational attribute types.

Annex G, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module which contains all the definitions associated with operational binding management operations.

Annex H, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module which contains all the definitions associated with enhanced security.

Annex I, which is not an integral part of this Recommendation | International Standard, summarizes the mathematical terminology associated with tree structures.

Annex J, which is not an integral part of this Recommendation | International Standard, describes some criteria that can be considered in designing names.

Annex K, which is not an integral part of this Recommendation | International Standard, provides some examples of various aspects of Schema.

Annex L, which is not an integral part of this Recommendation | International Standard, provides an overview of the semantics associated with Basic Access Control permissions.

Annex M, which is not an integral part of this Recommendation | International Standard, provides an extended example of the use of Basic Access Control.

Annex N, which is not an integral part of this Recommendation | International Standard, describes some DSA specific entry combinations.

Annex O, which is not an integral part of this Recommendation | International Standard, provides a framework for the modelling of knowledge.

Annex P, which is not an integral part of this Recommendation | International Standard, describes criteria on whether a name can be an alternative distinguished name or the primary distinguished name, whether it can contain alternative values, and whether it can include context information.

Annex Q, which is not an integral part of this Recommendation | International Standard, describes the concept of subfilters.

Annex R, which is not an integral part of this Recommendation | International Standard, describes recommendations and examples on how family members can be named.

Annex S, which is not an integral part of this Recommendation | International Standard, gives an introduction to Naming Concepts and Considerations.

Annex T, which is not an integral part of this Recommendation | International Standard, lists alphabetically the terms defined in this Recommendation | International Standard.

Annex U, 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.

**INTERNATIONAL STANDARD
ITU-T RECOMMENDATION**

**Information technology – Open Systems Interconnection –
The Directory: Models**

SECTION 1 – GENERAL

1 Scope

The models defined in this Recommendation | International Standard provide a conceptual and terminological framework for the other ITU-T X.500-series Recommendations | parts of ISO/IEC 9594 which define various aspects of the Directory.

The functional and administrative authority models define ways in which the Directory can be distributed, both functionally and administratively. Generic DSA and DSA information models and an Operational Framework are also provided to support Directory distribution.

The generic Directory Information Models describe the logical structure of the DIB from the perspective of Directory and Administrative Users. In these models, the fact that the Directory is distributed, rather than centralized, is not visible.

This Recommendation | International Standard provides a specialization of the generic Directory Information Models to support Directory Schema administration.

The other ITU-T Recommendations in the X.500 series | parts of ISO/IEC 9594 make use of the concepts defined in this Recommendation | International Standard to define specializations of the generic information and DSA models to provide specific information, DSA and operational models supporting particular directory capabilities (e.g., Replication):

- a) the service provided by the Directory is described (in ITU-T Rec. X.511 | ISO/IEC 9594-3) in terms of the concepts of the information framework; this allows the service provided to be somewhat independent of the physical distribution of the DIB;
- b) the distributed operation of the Directory is specified (in ITU-T Rec. X.518 | ISO/IEC 9594-4) so as to provide that service, and therefore maintain that logical information structure, given that the DIB is in fact highly distributed;
- c) replication capabilities offered by the component parts of the Directory to improve overall Directory performance are specified (in ITU-T Rec. X.525 | ISO/IEC 9594-9).

The security model establishes a framework for the specification of access control mechanisms. It provides a mechanism for identifying the access control scheme in effect in a particular portion of the DIT, and it defines three flexible, specific access control schemes which are suitable for a wide variety of applications and styles of use. The security model also provides a framework for protecting the confidentiality and integrity of directory operations using mechanisms such as encryption and digital signatures. This makes use of the framework for authentication defined in ITU-T Rec. X.509 | ISO/IEC 9594-8 as well as generic upper layers security tools defined in ITU-T Rec. X.830 | ISO/IEC 11586-1.

DSA models establish a framework for the specification of the operation of the components of the Directory. Specifically:

- a) the Directory functional model describes how the Directory is manifested as a set of one or more components, each being a DSA;
- b) the Directory distribution model describes the principals according to which the DIB entries and entry-copies may be distributed among DSAs;
- c) the DSA information model describes the structure of the Directory user and operational information held in a DSA;
- d) the DSA operational framework describes the means by which the definition of specific forms of cooperation between DSAs to achieve particular objectives (e.g., shadowing) is structured.

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

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.
- ITU-T Recommendation X.500 (2008) | ISO/IEC 9594-1:2008, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.
- ITU-T Recommendation X.509 (2008) | ISO/IEC 9594-8:2008, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.511 (2008) | ISO/IEC 9594-3:2008, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.
- ITU-T Recommendation X.518 (2008) | ISO/IEC 9594-4:2008, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*.
- ITU-T Recommendation X.519 (2008) | ISO/IEC 9594-5:2008, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.
- ITU-T Recommendation X.520 (2008) | ISO/IEC 9594-6:2008, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- ITU-T Recommendation X.521 (2008) | ISO/IEC 9594-7:2008, *Information technology – Open Systems Interconnection – The Directory: Selected object classes*.
- ITU-T Recommendation X.525 (2008) | ISO/IEC 9594-9:2008, *Information technology – Open Systems Interconnection – The Directory: Replication*.
- ITU-T Recommendation X.530 (2008) | ISO/IEC 9594-10:2008, *Information technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory*.
- ITU-T Recommendation X.660 (2008) | ISO/IEC 9834-1:2008, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree*.
- ITU-T Recommendation X.680 (2008) | ISO/IEC 8824-1:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.681 (2008) | ISO/IEC 8824-2:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- ITU-T Recommendation X.682 (2008) | ISO/IEC 8824-3:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- ITU-T Recommendation X.683 (2008) | ISO/IEC 8824-4:2008, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.
- ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Access control framework*.
- ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems – Non-repudiation framework*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*.

2.3 Other references

- IETF RFC 4510 (2006), *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*.

Withdrawn