INTERNATIONAL STANDARD

ISO/IEC 9594-2

Ninth edition
2020-11

Information technology — Open systems interconnection —

Part 2: The Directory: Models

Reference number
ISO/IEC 9594-2:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by ITU-T as ITU-T X.501 (10/2019) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This ninth edition cancels and replaces the eighth edition (ISO/IEC 9594-2:2017), which has been technically revised.

A list of all parts in the ISO/IEC 9594 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2020 – All rights reserved

CONTENTS

Page

SECTION 1 – GENERAL 1
1 Scope 1
2 References 2
2.1 Normative references 2
2.2 Non-normative 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 5
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 7
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 name 23
9.4 Name matching 24
9.5 Distinguished names 24
9.6 Alias names 25
10 Hierarchical groups 25
10.1 Definitions 25
10.2 Hierarchical relationship 26
10.3 Sequential ordering of a hierarchical group 26
SECTION 4 – DIRECTORY ADMINISTRATIVE MODEL 28
11 Directory Administrative Authority model 28
11.1 Definitions 28

© ISO/IEC 2020 – All rights reserved

Page

11.2 Overview ... 28
11.3 Policy ... 29
11.4 Specific administrative authorities ... 29
11.5 Administrative areas and administrative points ... 30
11.6 DIT Domain policies ... 32
11.7 DMD policies ... 32

SECTION 5 – MODEL OF DIRECTORY ADMINISTRATIVE AND OPERATIONAL INFORMATION ... 34

12 Model of Directory Administrative and Operational Information ... 34
12.1 Definitions ... 34
12.2 Overview ... 34
12.3 Subtrees ... 35
12.4 Operational attributes ... 37
12.5 Entries ... 37
12.6 Subentries ... 38
12.7 Information model for collective attributes ... 39
12.8 Information model for context defaults ... 40

SECTION 6 – THE DIRECTORY SCHEMA ... 41

13 Directory Schema ... 41
13.1 Definitions ... 41
13.2 Overview ... 41
13.3 Object class definition ... 43
13.4 Attribute type definition ... 45
13.5 Matching rule definition ... 48
13.6 Relaxation and tightening ... 50
13.7 DIT structure definition ... 56
13.8 DIT content rule definition ... 59
13.9 Context type definition ... 60
13.10 DIT Context Use definition ... 61
13.11 Friends definition ... 62
13.12 Syntax definitions ... 63

14 Directory System Schema ... 63
14.1 Overview ... 63
14.2 System schema supporting the administrative and operational information model ... 63
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 ... 67
14.8 System schema supporting the service administration model ... 68
14.9 System schema supporting password administration ... 68
14.10 System schema supporting hierarchical groups ... 69
14.11 Maintenance of system schema ... 70
14.12 System schema for first-level subordinates ... 71

15 Directory schema administration ... 71
15.1 Overview ... 71
15.2 Policy objects ... 71
15.3 Policy parameters ... 71
15.4 Policy procedures ... 72
15.5 Subschema modification procedures ... 72
15.6 Entry addition and modification procedures ... 73
15.7 Subschema policy attributes ... 73

SECTION 7 – DIRECTORY SERVICE ADMINISTRATION ... 79

16 Service Administration Model ... 79

 © ISO/IEC 2020 – All rights reserved

Page

16.1 Definitions ... 79
16.2 Service-type/user-class model ... 79
16.3 Service-specific administrative areas ... 80
16.4 Introduction to search-rules ... 81
16.5 Subfilters ... 81
16.6 Filter requirements ... 82
16.7 Attribute information selection based on search-rules ... 82
16.8 Access control aspects of search-rules ... 83
16.9 Contexts aspects of search-rules ... 83
16.10 Search-rule specification ... 83
16.11 Matching restriction definition ... 91
16.12 Search-validation function ... 91

SECTION 8 – SECURITY ... 93

17 Security model ... 93
17.1 Definitions ... 93
17.2 Security policies ... 93
17.3 Protection of Directory operations ... 94

18 Basic Access Control ... 95
18.1 Scope and application ... 95
18.2 Basic Access Control model ... 95
18.3 Access control administrative areas ... 98
18.4 Representation of Access Control Information ... 100
18.5 ACI operational attributes ... 105
18.6 Protecting the ACI ... 106
18.7 Access control and Directory operations ... 106
18.8 Access Control Decision Function ... 106
18.9 Simplified Access Control ... 108

19 Rule-based Access Control ... 108
19.1 Scope and application ... 108
19.2 Rule-based Access Control model ... 108
19.3 Access control administrative areas ... 109
19.4 Security Label ... 109
19.5 Clearance ... 110
19.6 Access Control and Directory operations ... 111
19.7 Access Control Decision Function ... 111
19.8 Use of Rule-based and Basic Access Control ... 112

20 Data Integrity in Storage ... 112
20.1 Introduction ... 112
20.2 Protection of an Entry or Selected Attribute Types ... 112
20.3 Context for Protection of a Single Attribute Value ... 114

SECTION 9 – DSA MODELS ... 115

21 DSA Models ... 115
21.1 Definitions ... 115
21.2 Directory Functional Model ... 115
21.3 Directory Distribution Model ... 116

SECTION 10 – DSA INFORMATION MODEL ... 118

22 Knowledge ... 118
22.1 Definitions ... 118
22.2 Introduction ... 118
22.3 Knowledge References ... 119
22.4 Minimum Knowledge ... 121
22.5 First Level DSAs ... 121
22.6 Knowledge references to LDAP servers ... 122

© ISO/IEC 2020 – All rights reserved

Page

23 Basic Elements of the DSA Information Model 122
23.1 Definitions 122
23.2 Introduction 122
23.3 DSA Specific Entries and their Names 123
23.4 Basic Elements 124
24 Representation of DSA Information 125
24.1 Representation of Directory User and Operational Information 126
24.2 Representation of Knowledge References 126
24.3 Representation of Names and Naming Contexts 133
SECTION 11 – DSA OPERATIONAL FRAMEWORK 135
25 Overview 135
25.1 Definitions 135
25.2 Introduction 135
26 Operational bindings 135
26.1 General 135
26.2 Application of the operational framework 136
26.3 States of cooperation 137
27 Operational binding specification and management 138
27.1 Operational binding type specification 138
27.2 Operational binding management 139
27.3 Operational binding specification templates 139
28 Operations for operational binding management 141
28.1 Application-context definition 141
28.2 Establish Operational Binding operation 142
28.3 Modify Operational Binding operation 145
28.4 Terminate Operational Binding operation 147
28.5 Operational Binding Error 148
28.6 Operational Binding Management Bind and Unbind 149
SECTION 12 – INTERWORKING WITH LDAP 151
29 Overview 151
29.1 Definitions 151
29.2 Introduction 151
30 LDAP interworking model 151
30.1 LDAP interworking scenarios 151
30.2 Overview of bound DSA handling LDAP operations 152
30.3 General LDAP requestor characteristics 152
30.4 LDAP extension mechanisms 153
31 LDAP specific system schema 153
31.1 Operational Attribute types from IETF RFC 4512 153
Annex A – Object identifier usage 156
Annex B – Information framework in ASN.1 159
Annex C – Subschema administration in ASN.1 170
Annex D – Service administration in ASN.1 175
Annex E – Basic Access Control in ASN.1 179
Annex F – DSA operational attribute types in ASN.1 183
Annex G – Operational binding management in ASN.1 186
Annex H – Enhanced security in ASN.1 191
Annex I – LDAP system schema 194
Annex J – The mathematics of trees 196
Annex K – Name design criteria 197

 © ISO/IEC 2020 – All rights reserved

Page

Annex L – Examples of various aspects of schema 199
L.1 Example of an attribute hierarchy 199
L.2 Example of a subtree specification 199
L.3 Schema specification 200
L.4 DIT content rules 201
L.5 DIT context use 202
Annex M – Overview of basic access control permissions 203
M.1 Introduction 203
M.2 Permissions required for operations 203
M.3 Permissions affecting error 204
M.4 Entry level permissions 204
M.5 Entry level permissions 205
Annex N – Examples of access control 206
N.1 Introduction 206
N.2 Design principles for Basic Access Control 206
N.3 Introduction to example 207
N.4 Policy affecting the definition of specific and inner areas 208
N.5 Policy affecting the definition of Directory Access Control Domains (DACDs) 209
N.6 Policy expressed in prescriptiveACI attributes 212
N.7 Policy expressed in subentryACI attributes 216
N.8 Policy expressed in entryACI attributes 217
N.9 ACDF examples 218
N.10 Rule-based access control 220
Annex O – DSE type combinations 221
Annex P – Modelling of knowledge 223
Annex Q – Subfilters 227
Annex R – Compound entry name patterns and their use 228
Annex S – Naming concepts and considerations 230
S.1 History tells us … 230
S.2 A new look at name resolution 230
Annex T – Alphabetical index of definitions 236
Annex U – Amendments and corrigenda 238

© ISO/IEC 2020 – All rights reserved

Introduction

This Recommendation | International Standard, together with other Recommendations in the ITU-T X.500-series | parts of ISO/IEC 9594, 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 (OSI), 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 ninth edition technically revises and enhances the eighth edition of this Recommendation | International Standard.

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 an integral part of this Recommendation | International Standard, provides the ASN.1 module which contains the definitions for LDAP system schema using the ASN.1 ATTRIBUTE information object.

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

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

 © ISO/IEC 2020 – All rights reserved

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

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

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

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

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

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.

© ISO/IEC 2020 – All rights reserved

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 Directory System Agent (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 Directory Information Base (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 Rec. ITU-T 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 Rec. ITU-T 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 Rec. ITU-T 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 Directory Information Tree (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 Rec. ITU-T X.509 | ISO/IEC 9594-8 as well as generic upper layers security tools defined in Rec. ITU-T 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.

© ISO/IEC 2020 – All rights reserved

2 References

2.1 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.

2.1.1 Identical Recommendations | International Standards

- Recommendation ITU-T X.500 (2019) | ISO/IEC 9594-1:2020, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services*.
- Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8:2020, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- Recommendation ITU-T X.511 (2019) | ISO/IEC 9594-3:2020, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition*.
- Recommendation ITU-T X.518 (2019) | ISO/IEC 9594-4:2020, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation*.
- Recommendation ITU-T X.519 (2019) | ISO/IEC 9594-5:2020, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications*.
- Recommendation ITU-T X.520 (2019) | ISO/IEC 9594-6:2020, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- Recommendation ITU-T X.521 (2019) | ISO/IEC 9594-7:2020, *Information technology – Open Systems Interconnection – The Directory: Selected object classes*.
- Recommendation ITU-T X.525 (2019) | ISO/IEC 9594-9:2020, *Information technology – Open Systems Interconnection – The Directory: Replication*.
- Recommendation ITU-T X.660 (2011) | ISO/IEC 9834-1:2012, *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.*
- Recommendation ITU-T X.680 (2015) | ISO/IEC 8824-1:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- Recommendation ITU-T X.681 (2015) | ISO/IEC 8824-2:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- Recommendation ITU-T X.682 (2015) | ISO/IEC 8824-3:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- Recommendation ITU-T X.683 (2015) | ISO/IEC 8824-4:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- Recommendation ITU-T X.690 (2015) | ISO/IEC 8825-1:2015, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

2.1.2 Paired Recommendations | International Standards equivalent in technical content

- Recommendation ITU-T X.800 (1991) (previously CCITT Recommendation), *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*.

2.1.3 Other references

- IETF RFC 4510 (2006), *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map.*
- IETF RFC 4511 (2006), *Lightweight Directory Access Protocol (LDAP): The Protocol.*
- IETF RFC 4512 (2006), *Lightweight Directory Access Protocol (LDAP): Directory Information Models*.

 © ISO/IEC 2020 – All rights reserved