INTERNATIONAL STANDARD

ISO/IEC 9594-2

Information technology — Open Systems Interconnection — The Directory: Models

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — L'Annuaire: Modèles

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 9594-2:1995
https://standards.iteh.ai/catalog/standards/sist/2bc2335b-e64a-4d41-9e88-
7725c08cc2bc/iso-iec-9594-2-1995

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. 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.

International Standard ISO/IEC 9594-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing,* in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.501.

Implementors should note that a defect resolution process exists and that corrections may be applied to this part of ISO/IEC 9594 in the form of technical corrigenda. A list of approved technical corrigenda for this part of ISO/IEC 9594 can be obtained from the subcommittee secretariat. Published technical corrigenda are available from your national standards organization.

This second edition technically revises and enhances ISO/IEC 9594-2:1990. It also incorporates technical corrigendum 1:1991 and technical corrigendum 2:1992. Implementations may still claim conformance to the first edition of this part of ISO/IEC 9594. However, at some point, the first edition will no longer be supported (i.e. reported defects will no longer be resolved). It is recommended that implementations conform to this second edition as soon as possible.

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: Authentication framework*

— *Part 9: Replication*

Annexes A to F form an integral part of this part of ISO/IEC 9594. Annexes G to O are for information only.

Introduction

This Recommendation I International Standard, together with the other Recommendation I 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 which 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 I 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 I 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 I International Standard provides a specialization of the generic Directory Information Models to support Directory Schema administration.

This second edition technically revises and enhances, but does not replace, the first edition of this Recommendation I International Standard. Implementations may still claim conformance to the first edition.

This second edition specifies version 1 of the Directory service and protocols. The first edition also specifies version 1. Differences between the services and between the protocols defined in the two editions are accommodated using the rules of extensibility defined in this edition of X.519 I ISO/IEC 9594-5.

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

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

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

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

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

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

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

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

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

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

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

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

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

Annex O, which is not an integral part of this Recommendation I International Standard, lists the amendments and defect reports that have been incorporated to form this edition of this Recommendation I 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 I International Standard provide a conceptual and terminological framework for the other ITU-T X.500 Series Recommendations I 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 I 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 I parts of ISO/IEC 9594 make use of the concepts defined in this Recommendation I 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 I 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 I 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 I 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 two flexible, specific access control schemes which are suitable for a wide variety of applications and styles of use. The security model is concerned solely with control of access to the Directory information, not control of access to the DSA application-entity holding the information.

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 I International Standard part. 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 I International Standard are encouraged to investigate the possibility of applying the most recent editions 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 I International Standards

– ITU-T Recommendation X.500 (1993) I ISO/IEC 9594-1:1995, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.*

– ITU-T Recommendation X.509 (1993) I ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*

– ITU-T Recommendation X.511 (1993) I ISO/IEC 9594-3:1995, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition.*

– ITU-T Recommendation X.518 (1993) I ISO/IEC 9594-4:1995, *Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation.*

– ITU-T Recommendation X.519 (1993) I ISO/IEC 9594-5:1995, *Information technology – Open Systems Interconnection –The Directory: Protocol specifications.*

– ITU-T Recommendation X.520 (1993) I ISO/IEC 9594-6:1995, *Information technology – Open Systems Interconnection –The Directory: Selected attribute types.*

– ITU-T Recommendation X.521 (1993) I ISO/IEC 9594-7:1995, *Information technology – Open Systems Interconnection –The Directory: Selected object classes.*

– ITU-T Recommendation X.525 (1993) I ISO/IEC 9594-9:1995, *Information technology – Open Systems Interconnection – The Directory: Replication.*

– ITU-T Recommendation X.680 (1994) I ISO/IEC 8824-1:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

– ITU-T Recommendation X.681 (1994) I ISO/IEC 8824-2:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*

– ITU-T Recommendation X.682 (1994) I ISO/IEC 8824-3:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*

– ITU-T Recommendation X.683 (1994) I ISO/IEC 8824-4:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

– ITU-T Recommendation X.811[1] I ISO/IEC 10181-1:...[1], *Information technology – Open Systems Interconnection – Security Frameworks in Open Systems: Authentication framework.*

– ITU-T Recommendation X.812[1] I ISO/IEC 10181-2:...[1], *Information technology – Open Systems Interconnection – Security Frameworks in Open Systems – Access control framework.*

– ITU-T Recommendation X.813[1] I ISO/IEC 10181-3:...[1], *Information technology – Open Systems Interconnection – Security Frameworks in Open Systems – Non-repudiation framework.*

2.2 Paired Recommendations I International Standards equivalent in technical content

– CCITT Recommendation X.200 (1988), *Reference Model of Open Systems Interconnection for CCITT Applications.*

– ISO 7498:1984, *Information processing systems –Open Systems Interconnection – Basic Reference Model.*

– 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.*

---

[1] Presently at the stage of draft.

3 Definitions

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

3.1 OSI Reference Model Definitions

The following terms are defined in CCITT Rec. X.200 | ISO 7498:

    a)   *application-context;*

    b)   *application-entity;*

    c)   *application-process.*

3.2 Basic directory definitions

The following terms are defined in ITU-T Rec. X.500 | ISO/IEC 9594-1:

    a)   *Directory;*

    b)   *Directory Access Protocol;*

    c)   *Directory Information Base;*

    d)   *Directory Operational Binding Protocol;*

    e)   *Directory System Protocol;*

    f)   *(Directory) user.*

3.3 Distributed operation definitions

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

    a)   *access point;*

    b)   *hierarchical operational binding;*

    c)   *name resolution;*

    d)   *non-specific hierarchical operational binding;*

    e)   *relevant hierarchical operational binding.*

3.4 Replication definitions

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

    a)   *cache-copy;*

    b)   *consumer reference;*

    c)   *entry-copy;*

    d)   *master DSA;*

    e)   *primary shadowing;*

    f)   *replicated area;*

    g)   *replication;*

    h)   *secondary shadowing;*

    i)   *shadow consumer;*

    j)   *shadow supplier;*

    k)   *Shadowed DSA-Specific Entry;*

    l)   *shadowing;*

    m) *supplier reference.*

The definitions of terms defined in this Recommendation | International Standard are included at the beginning of individual clauses, as appropriate. An index of these terms is provided in Annex N for easy reference.

4 Abbreviations

ACDF	Access Control Decision Function
ACI	Access Control Information
ACIA	Access Control Inner Area
ACSA	Access Control Specific Area
ADDMD	Administration Directory Management Domain
ASN.1	Abstract Syntax Notation 1
AVA	attribute value assertion
BER	(ASN.1) Basic Encoding Rules
DACD	Directory Access Control Domain
DAP	Directory Access Protocol
DIB	Directory Information Base
DISP	Directory Information Shadow Protocol
DIT	Directory Information Tree
DMD	Directory Management Domain
DMO	Domain Management Organization
DOP	Directory Operational Binding Management Protocol
DSA	Directory System Agent
DSE	DSA-Specific Entry
DSP	Directory System Protocol
DUA	Directory User Agent
HOB	Hierarchical Operational Binding
NHOB	Non-specific Hierarchical Operational Binding
NSSR	Non-Specific Subordinate Reference
PRDMD	Private Directory Management Domain
RHOB	Relevant Hierarchical Operational Binding (i.e. either a HOB or NHOB, as appropriate)
RDN	Relative Distinguished Name
SDSE	Shadowed DSE

5 Conventions

With minor exceptions this Directory Specification has been prepared according to the "Presentation of ITU-T/ISO/IEC common text" guidelines in the Guide for ITU-T and ISO/IEC JTC 1 Cooperation, March 1993.

The term "Directory Specification" (as in "this Directory Specification") shall be taken to mean ITU-T Rec. X.501 | ISO/IEC 9594-2. The term "Directory Specifications" shall be taken to mean the X.500-Series Recommendations and all parts of ISO/IEC 9594.

This Directory Specification uses the term "1988 edition systems" to refer to systems conforming to the previous (1988) edition of the Directory Specifications, i.e. the 1988 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:1990 edition. Systems conforming to the current Directory Specifications are referred to as "1993 edition systems".

SECTION 2 – OVERVIEW OF THE DIRECTORY MODELS

6 Directory Models

6.1 Definitions

For the purposes of this Directory Specification, the following definitions apply:

6.1.1 administrative authority: An agent of the Domain Management Organization concerned with various aspects of Directory administration. The term *administrative authority* (in lower case) refers to the power vested in an Administrative Authority by the Domain Management Organization to execute policy.

6.1.2 administration directory management domain (ADDMD): A DMD which is managed by an Administration.

NOTE 1 – The term Administration denotes a public telecommunications administration or other organization offering public telecommunications services.

6.1.3 directory administrative and operational information: Information used by the Directory for administrative and operational purposes.

6.1.4 DIT domain: That part of the global DIT held by the DSAs- forming a DMD.

6.1.5 directory management domain (DMD): A set of one or more DSAs and zero or more DUAs managed by a single organization.

6.1.6 domain management organization: An organization that manages a DMD (and the associated DIT Domain).

6.1.7 directory user information: Information of interest to users and their applications.

6.1.8 directory system agent (DSA): An OSI application process which is part of the Directory.

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

6.1.10 directory user agent (DUA): An OSI application process which represents a user in accessing the Directory.

NOTE 2 – DUAs may also provide a range of local facilities to assist users compose queries and interpret the responses.

6.1.11 private directory management domain (PRDMD): A DMD which is managed by an organization other than an Administration.

6.2 The Directory and its Users

The *Directory* is a repository of information. This repository is known as the Directory Information Base (DIB). Directory services provided to users are concerned with various kinds of access to this information.

The services provided by the Directory are defined in ITU-T Rec. X.511 | ISO/IEC 9594-3.

A Directory user (e.g. a person or an application-process) obtains Directory services by accessing the Directory. More precisely, a *Directory User Agent (DUA)* actually accesses the Directory and interacts with it to obtain the service on behalf of a particular user. The Directory provides one or more *access points* at which such accesses can take place. These concepts are illustrated in Figure 1.

A DUA is manifested as an application-process. In any instance of communication each DUA represents precisely one directory user.

The Directory is manifested as a set of one or more application-processes known as *Directory System Agents (DSAs)*, each of which provides one or more of the access points. For a more detailed description of DSAs see 17.2.

NOTES

1 Some open systems may provide a centralized DUA function retrieving information for the actual users (application-processes, persons, etc.). This is transparent to the Directory.

2 The DUA functions and a DSA can be within the same open system, and it is an implementation choice whether to make one or more DUAs visible within the OSI Environment as application-entities.

3 A DUA may exhibit local behavior and structure which is outside the scope of envisaged Directory Specifications For example, a DUA which represents a human directory user may provide a range of local facilities to assist its user to compose queries and interpret the responses.
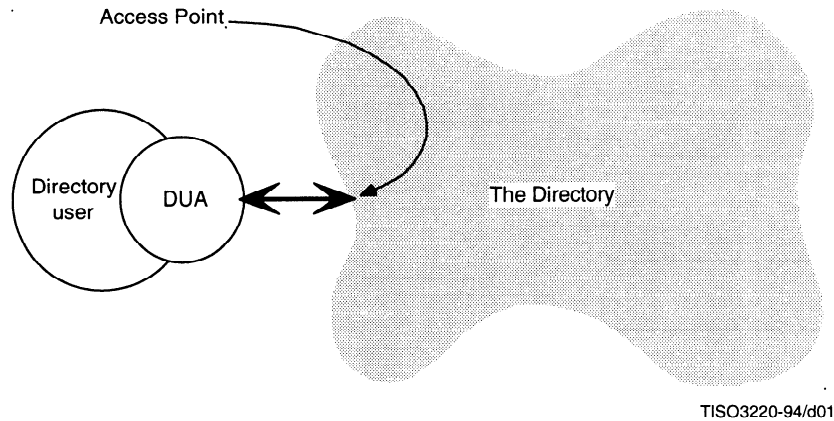
TISO3220-94/d01

Figure 1 – Access to the Directory

6.3 Directory and DSA Information Models

6.3.1 Generic Models

Directory information may be classified as either:

- user information, placed in the Directory by, or on behalf of, users; and subsequently administered by, or on behalf of, users. Section 3 provides a model of this information, or;

- administrative and operational information, held by the Directory to meet various administrative and operational requirements. Section 5 provides a model of this information. Also provided in Section 5 is a specification of the relationship between the user, administrative and operational information models.

These models, presenting views of the DIB from different perspectives, are referred to as the generic Directory Information Models.

Directory information models describe how the Directory as a whole represents information. The composition of the Directory as a set of potentially cooperating DSAs is abstracted from the model. The DSA information model, on the other hand, is especially concerned with DSAs and the information that must be held by DSAs in order that the set of DSAs comprising the Directory may together realize the Directory information model. The DSA Information Model is provided in clauses 18 through 20.

The DSA information model is a generic model describing the information held by DSAs and the relationship between this information and the DIB and DIT.

Some, but not all, of the information represented by the DSA information model is accessible via the Directory abstract service. Therefore, administration of all of the information described in these Directory Specifications is not possible via the Directory abstract service. It is envisioned that administration of DSA information will initially be a local matter, but that eventually some generic system management service will be employed to provide access to all of the information described in the DSA information model.

6.3.2 Specific Information Models

Subsequent to the development of generic models for the Directory as a whole and for its components, specific information models are required for the standardisation of particular aspects of the operation of the Directory and its components.

The generic Directory Information Models establish a framework for the following specific information models:

- an access control information model;

- a subschema information model;

- a collective attribute information model.

The generic DSA Information Model in turn establishes a framework for the following specific information models:

- a model for a DSA's distribution knowledge;

- a model for a DSA's replication knowledge.

6.4 Directory Administrative Authority Model

A Directory Management Domain (DMD) is a set of one or more DSAs and zero or more DUAs managed by a single organization.

That part of the global DIT held by (the DSAs forming) a DMD is referred to as a *DIT Domain*. There is a one to one correspondence between DMDs and DIT Domains. The term DMD is used when referring to the management of the functional components of the Directory. The term DIT Domain is used when referring to the management of Directory Information. Two important points regarding this terminology are:

- A DIT Domain consists of one or more disjoint subtrees of the DIT (see 10.5). A DIT Domain shall not contain the root of the global DIT.

- The term DMD may also be used as a general term when both aspects of management are considered together.

An organization that manages a DMD (and the associated DIT Domain) is referred to as a *Domain Management Organization (DMO)*.

NOTE – A DMO may be an Administration (i.e. a public telecommunications administration or other organization offering public telecommunications services) in which case the managed DMD is said to be an Administration DMD (ADDMD); otherwise it is a Private DMD (PRDMD). It should be recognized that the provision of support for private directory systems by ITU-T members falls within the framework of national regulations. Thus, the technical possibilities described may or may not be offered by an Administration which provides directory services. The internal operation and configuration of private DMDs is not within the scope of envisaged Directory Specifications.

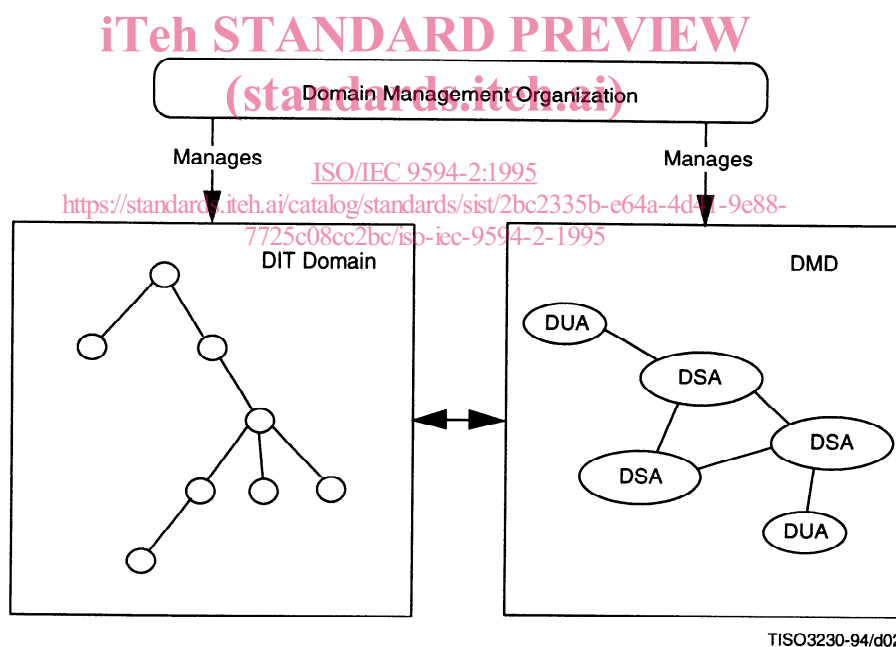Figure 2 illustrates the relationship between a DMO, DMD and DIT Domain.

Figure 2 – Directory Management

Management of a DUA by a DMO implies an ongoing responsibility for service to that DUA, e.g. maintenance, or in some cases ownership, by the DMO. The DMO may or may not elect to make use of the Directory Specifications to govern any interactions among DUAs and DSAs which are wholly within the DMD.

An agent of a DMO concerned with various aspects of Directory administration is referred to as an *Administrative Authority*. The term *administrative authority* (in lower case) refers to the power vested in an Administrative Authority by a DMO to execute policy.

NOTE – A Directory Administrative Authority Model is specified in Section 4.