INTERNATIONAL STANDARD

ISO/IEC 9594-4

Ninth edition
2020-11

Information technology — Open systems interconnection —

Part 4: The Directory: Procedures for distributed operation

Reference number
ISO/IEC 9594-4:2020(E)

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.518 (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 9594-4:2017), 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.

CONTENTS

Introduction

This Recommendation | International Standard, together with other Recommendations | International Standards, have 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 specifies the procedures by which the distributed components of the Directory interwork in order to provide a consistent service to its users.

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.

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

Rec. ITU-T X.511 (1993) | ISO/IEC 9594-3 (1995), Rec. ITU-T X.518 (1993) | ISO/IEC 9594-4 (1995) and Rec. ITU-T X.519 (1993) | ISO/IEC 9594-5 (1995) and their previous edition 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 nine 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, provides the ASN.1 module for directory distributed operations.

Annex B, which is an integral part of this Recommendation | International Standard, provides the ASN.1 module providing definitions for hierarchical operational bindings.

Annex C, which is not an integral part of this Recommendation | International Standard, describes an example of distributed name resolution.

Annex D, which is not an integral part of this Recommendation | International Standard, describes authentication in the distributed operations environment.

Annex E, which is not an integral part of this Recommendation | International Standard, illustrates knowledge maintenance.

Annex F, 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 ISO/IEC 9594-4
RECOMMENDATION ITU-T X.518

Information technology – Open Systems Interconnection – The Directory: Procedures for distributed operation

SECTION 1 – GENERAL

1 Scope

This Recommendation | International Standard specifies the behaviour of DSAs taking part in a distributed directory consisting of multiple Directory systems agents (DSAs) and/or LDAP servers with at least one DSA. The allowed behaviour has been designed to ensure a consistent service given a wide distribution of the DIB across a distributed directory. Only the behaviour of DSAs taking part in a distributed directory is specified. The behaviour of LDAP servers are specified in relevant LDAP specifications. There are no special requirements on an LDAP server beyond those given by the LDAP specifications.

The Directory is not intended to be a general purpose database system, although it may be built on such systems. It is assumed that there is a considerably higher frequency of queries than of updates.

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.501 (2019) | ISO/IEC 9594-2:2020, *Information technology – Open Systems Interconnection – The Directory: Models*.
- 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.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.680 (2015) | ISO/IEC 8824-1:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

2.1.2 Other references

- 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*.
- IETF RFC 4511 (2006), *Lightweight Directory Access Protocol (LDAP): The Protocol*.
- IETF RFC 4514 (2006), *Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*.

2.2 Non-normative reference

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

3 Definitions

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

3.1 Basic Directory definitions

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

a) *(the) Directory*;

b) *Directory Information Base*.

3.2 Directory model definitions

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

a) *access point*;

b) *alias*;

c) *Directory Information Tree* ;

d) *Directory System Agent (DSA)*;

e) *Directory User Agent (DUA)*;

f) *distinguished name*;

g) *relative distinguished name*.

3.3 DSA information model definitions

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

a) *category*;

b) *commonly usable*;

c) *context prefix*;

d) *cross reference*;

e) *DIB fragment*;

f) *DSA information tree*;

g) *DSA-Specific Entry (DSE)*;

h) *DSE type*;

i) *immediate superior reference*;

j) *knowledge information*;

k) *knowledge reference category*;

l) *knowledge reference type*;

m) *naming context*;

n) *non-specific knowledge*;

o) *non-specific subordinate reference*;

p) *operational attribute*;

q) *reference path*;

r) *specific knowledge*;

s) *subordinate reference*;

t) *superior reference*.

3.4 Abstract service definitions

The following terms are defined in Rec. ITU-T X.511 | ISO/IEC 9594-3:

a) *reply*;

b) *request*;

c) *requester*.

3.5 Protocol definitions

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

a) *application-association*;

b) *application-entity-title*.

3.6 Directory replication definitions

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

a) *attribute completeness*;

b) *shadowing operational binding*;

c) *subordinate completeness*;

d) *unit of replication*.

3.7 Distributed operation definitions

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

3.7.1 **base object**: The object or alias entry that is the target for an operation as issued by the requester.

3.7.2 **bound DSA**: The DSA to which the requesting DUA or LDAP client has bound, by having performed a Bind operation with that DSA.

3.7.3 **bound-DSA paged results**: The paging is performed entirely by the DSA to which the DUA is bound.

NOTE – This is the only mode of paging supported by systems conforming to Rec. ITU-T X.518 (2001) | ISO/IEC 9594-4:2001 or prior editions.

3.7.4 **chaining**: The generic term for uni-chaining or multi-chaining.

3.7.5 **context prefix information**: Operational and user information supplied by the superior DSA to the subordinate DSA in an RHOB regarding DIT vertices superior to the subordinate context prefix.

3.7.6 **directory server**: A DSA or an LDAP server.

3.7.7 **distributed directory**: An interconnected set of directory servers where at least one directory server shall be a DSA.

3.7.8 **distributed name resolution**: The process by which name resolution starts in a DSA and continues in one or more Directory servers.

3.7.9 **DSP paged results**: The DSP protocol provisions when a performing DSA is different from a bound DSA, whereby paged results by the initial performer are accomplished.

3.7.10 **error**: Information sent from the performer to the requester conveying a negative outcome of a previously received request.

3.7.11 **hard error**: A definite error which indicates that the operation cannot currently be performed without external intervention.

3.7.12 **hierarchical operational binding (HOB)**: Relationship between two master DSAs holding naming contexts, one of which is immediately subordinate to the other, in which the superior DSA holds a subordinate reference to the subordinate DSA.

3.7.13 **initial performer**: The first DSA or LDAP server to start performing on an operation, i.e., the first DSA or LDAP server to enter the evaluation phase of the operation.

3.7.14 **LDAP requester**: A DSA that has the ability to access an LDAP server by using the LDAP protocol.

3.7.15 **modification operations**: These are the Directory Modify operations, i.e., Modify Entry, Add Entry, Remove Entry, Modify DN, Change Password and Administer Password operations.

3.7.16 **multi-chaining**: A mode of interaction in which a DSA processing a request itself sends multiple requests either in parallel or sequentially to a set of other DSAs.

3.7.17 **multiple entry interrogation operations**: These are the Directory Search operations, i.e., List and Search operations.

3.7.18 **name resolution**: The process of locating an entry by sequentially matching each RDN in a purported name to a vertex of the DIT.

3.7.19 **non-specific hierarchical operational binding (NHOB)**: Relationship between two master DSAs holding naming contexts, one of which is immediately subordinate to the other, in which the superior DSA holds a non-specific subordinate reference to the subordinate DSA.

3.7.20 **NSSR decomposition**: Decomposition of non-specific knowledge references into subrequests for other DSAs to pursue; these subrequests may be either chained to these DSAs by the DSA performing the decomposition, or a continuation reference identifying the DSAs may be returned to the requester for it to pursue, or the decomposing DSA may pursue some of the subrequests, leaving others unexplored for the requester to pursue.

3.7.21 **operation progress**: A set of values which denotes the extent to which name resolution has taken place.

3.7.22 **paging**: A `search` or `list` result is returned piecewise in the form of one or more pages that are comprised by a limited number of entries.

3.7.23 **performer**: DSA receiving a request (i.e., to perform an operation).

NOTE – The performer is also the initial performer except possibly for operations that involve more than one DSA for their evaluation.

3.7.24 **procedure**: An (informal) specification of how a DSA maps a given set of input arguments and its DSA information tree into a result.

NOTE – Input arguments and results may correspond to information received in a requested operation and information sent in a reply, or they may represent intermediate stages in the computation of a reply from a requested operation. In clause 14.2, the former variety of input arguments and results are termed external.

3.7.25 **relevant hierarchical operational binding (RHOB)**: Either an HOB or an NHOB, depending on the context.

3.7.26 **referral**: An outcome which can be returned by a DSA or LDAP server which cannot perform an operation itself, and which identifies one or more other DSAs or LDAP servers more able to perform the operation.

3.7.27 **request decomposition**: Decomposition by a DSA of a request into subrequests for other Directory servers to pursue; these subrequests may be either chained to these Directory servers by the DSA performing the decomposition, or continuation references identifying the Directory servers may be returned to the requester for it to pursue, or the decomposing DSA may pursue some of the subrequests, leaving others unexplored for the requester to pursue.

3.7.28 **single entry interrogation operations**: These are the Directory Read operations, i.e., Read and Compare operations.

3.7.29 **soft error**: An error which may be transient, or which may indicate a localized problem, in which case the use of a different knowledge reference or access point may enable a result or hard error to be obtained.

3.7.30 **subordinate DSA**: Of the two DSAs sharing an HOB or an NHOB, the DSA holding the subordinate naming context.

3.7.31 **subrequest**: A request generated by request decomposition.

3.7.32 **superior DSA**: Of the two DSAs sharing an HOB or an NHOB, the DSA holding the superior naming context.

3.7.33 superior, subordinate DSA: Two master DSAs holding naming contexts, one of which is immediately subordinate to the other; the relationship between the two DSAs is managed explicitly via an HOB (or NHOB), or exists implicitly by virtue of the superior DSA holding a subordinate (or non-specific subordinate) reference to the subordinate DSA.

3.7.34 target object name: The name of an entry either to which the operation is to be directed at a particular stage of name resolution, or which is involved in the evaluation of the operation.

3.7.35 uni-chaining: A mode of interaction optionally used by a DSA which cannot perform an operation itself. The DSA *chains* by invoking an operation of another DSA or LDAP server and then relaying the outcome to the original requester.

4 Abbreviations

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

ASN.1	Abstract Syntax Notation One
DAP	Directory Access Protocol
DIB	Directory Information Base
DISP	Directory Information Shadowing Protocol
DMD	Directory Management Domain
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
LDAP	Lightweight Directory Access Protocol
NHOB	Non-specific Hierarchical Operational Binding
NSSR	Non-Specific Subordinate Reference
RHOB	Relevant Hierarchical Operational Binding

5 Conventions

The term "Directory Specification" (as in "this Directory Specification") shall be taken to mean Rec. ITU-T X.518 | ISO/IEC 9594-4. The term "Directory Specifications" shall be taken to mean the Rec. ITU-T X.500-series | ISO/IEC 9594-1, Rec. ITU-T X.501 | IO/IEC 9594-2, Rec. ITU-T X.511 | ISO/IEC 9594-3, Rec. ITU-T X.518 | ISO/IEC 9594-4, Rec. ITU-T X.519 | ISO/IEC 9594-5, Rec. ITU-T X.520 | ISO/IEC 9594-6, Rec ITU-T X.521 | ISO/IEC 9594-7 and Rec. ITU-T X.525 | ISO/IEC 9594-9.

If an International Standard or ITU-T Recommendation is referenced within normal text without an indication of the edition, the edition shall be taken to be the latest one as specified in the normative references clause.

Prior to year 2020, the parts making up the Directory Specifications progressed together and can therefore collectively be identified as the Directory Specifications of a specific edition using the format: Rec. ITU-T X.5** (yyyy) | ISO/IEC 9594-*:yyyy (e.g.; Rec ITU-T X.5** (1993) | ISO/IEC 9594-*:1995).

This Directory Specification makes extensive use of Abstract Syntax Notation One (ASN.1) for the formal specification of data types and values, as it is specified in Rec. ITU-T X.680 | ISO/IEC 8824-1, ITU-T X.681 (2015) | ISO/IEC 8824-2, ITU-T X.682 (2015) | ISO/IEC 8824-3, ITU-T X.683 (2015) | ISO/IEC 8824-4 and Rec. ITU-T X.690 | ISO/IEC 8825-1.

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.

If the items in a list are numbered (as opposed to using "–" or letters), then the items shall be considered steps in a procedure.

SECTION 2 – OVERVIEW

6 Overview

The Directory abstract service allows the interrogation, retrieval and modification of Directory information in the DIB. This service is specified in in Rec. ITU-T X.511 | ISO/IEC 9594-3. Similarly, the lightweight directory access protocol (LDAP) allows the interrogation, retrieval and modification of Directory information in the DIB. This protocol and the services it enables are specified in IETF RFC 4511.

The abstract service as specified in Rec. ITU-T X.511 | ISO/IEC 9594-3 does not address the specification of Directory system agents (DSA) within which the DIB is stored and managed, and through which the service is provided. Furthermore, it does not consider whether the DIB is centralized, i.e., contained within a single DSA, or distributed over a DSA and a number of additional DSAs and/or LDAP servers. Directory server is the common name for a DSA or an LDAP server. Consequently, the requirements for DSAs to have knowledge of, navigate to and cooperate with other DSAs and or LDAP servers, in order to support the abstract service in a distributed environment is also not covered by the abstract service specification.

This Directory Specification specifies how a set of one or more DSAs and zero or more LDAP servers collectively constitute the distributed directory service.

In addition, this Directory Specification specifies the permissible ways in which the DIB may be distributed over one or more DSAs and zero or more LDAP servers. For the limiting case where the DIB is contained within a single DSA, the Directory is in fact centralized; for the case where the DIB is distributed over two or more DSAs, knowledge and navigation mechanisms are specified which ensure that the whole of the DIB is potentially accessible from all DSAs that hold constituent entries.

Portions of the DIB may also be replicated in multiple DSAs. The protocols described in this Directory Specification allow the use of replicated information to improve the availability, performance and efficiency of the distributed directory service. The use of replicated information is, to some extent, under the user's control, through the use of service control options. The procedures described in this Directory Specification also indicate some of the opportunities for design optimizations when using the replicated information.

Additionally, request handling interactions are specified that enable particular operational characteristics of the Directory to be controlled by its users. In particular, the user has control over whether a DSA, responding to a directory inquiry pertaining to information held in other directory server(s), has the option of interrogating the other DSA(s) directly (chaining) or, whether it should respond with information about other directory server(s) which could further progress the inquiry (referral).

Generally, the decision by a DSA to chain or refer is determined by the service controls set by the user, and by the DSA's own administrative, operational or technical circumstances.

Recognizing that, in general, the Directory will be distributed, and that directory inquiries will be satisfied by an arbitrary number of cooperating DSAs which may arbitrarily chain or refer according to the above criteria, this Directory Specification specifies the appropriate procedures to be effected by DSAs in responding to distributed directory inquiries. These procedures will ensure that users of the distributed Directory service perceive it to be both user-friendly and consistent.

NOTE – Although an LDAP server may participate in a distributed operation, it is not aware of this cooperation.

SECTION 3 – DISTRIBUTED DIRECTORY MODELS

7 Distributed Directory system model

The Directory abstract service, as defined in Rec. ITU-T X.511 | ISO/IEC 9594-3, models the Directory as an entity which provides a set of directory services to its users. Users of the Directory access its services through an access point.

Figure 1 illustrates the distributed directory model which will be used as the basis for specifying the distributed aspects of the directory. It illustrates the Directory as comprising a set of one or more DSAs and zero or more LDAP servers.

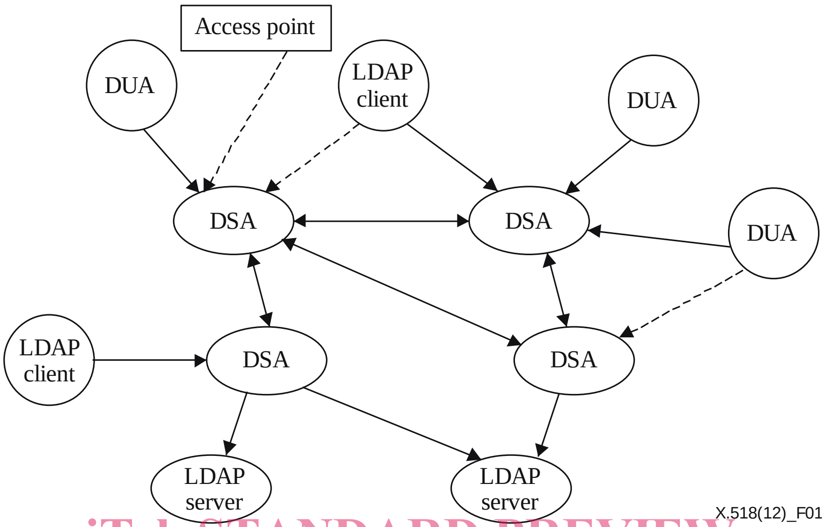

Figure 1 – The distributed directory model

DSAs are specified in detail in the subsequent clauses of this Directory Specification. This clause merely states a number of their characteristics, in order to serve as an introduction and to establish the relationship between this Directory Specification and the other Directory Specifications.

DSAs are defined in order that distribution of the DIB can be accommodated and that a number of physically distributed DSAs and LDAP servers can interact in a prescribed, cooperative manner to provide directory services to the users of the directory (DUAs and/or LDAP clients).

Figure 1 illustrates the relationship between the directory abstract service and the DSA abstract service. The directory abstract service defined in Rec. ITU-T X.511 | ISO/IEC 9594-3 is provided through a number of Directory operations. To realize this service, the DSAs and LDAP servers that comprise the Directory interact with one another. The nature of this interaction is defined in terms of the service that one DSA may provide to another DSA, the DSA abstract service. In addition, a DSA may interact with an LDAP server using the LDAP protocol as defined by IETF RFC 4511. When doing this, the DSA is called an *LDAP requester* and the DSA abstract service does not apply for this type of interaction. A DSA that is directly bound to a DUA or LDAP client is called the *bound DSA* (for that DUA or LDAP client).

As indicated in Figure 1, each of two interacting DSAs may provide a DSA abstract service to the other DSA. However, an LDAP server is not able to send requests to a DSA or to another LDAP server. LDAP servers are therefore always at the edge of the infrastructure.

The DSA abstract service is provided through a number of operations, termed chained operations, each having a counterpart in the Directory abstract service. Thus, a given operation in the directory abstract service, e.g., Read, may require that the DSA providing the service interact with one or more other DSAs using chained operations, e.g., Chained Read.

A DUA or LDAP client can only access the Directory by interacting with a DSA.

NOTE – An LDAP client interaction with an LDAP server is specified by IETF RFC 4510 and is outside the scope of these Directory Specifications.