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

*Technologies de l'information — Interconnexion de systèmes ouverts
(OSI) — L'annuaire: Procédures pour le fonctionnement réparti*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 9594-4:2005](https://standards.iteh.ai/catalog/standards/sist/834d129d-e44f-4cb9-8826-85b8426c5640/iso-iec-9594-4-2005)

<https://standards.iteh.ai/catalog/standards/sist/834d129d-e44f-4cb9-8826-85b8426c5640/iso-iec-9594-4-2005>

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 9594-4:2005](https://standards.iteh.ai/catalog/standards/sist/834d129d-e44f-4cb9-8826-85b8426c5640/iso-iec-9594-4-2005)

<https://standards.iteh.ai/catalog/standards/sist/834d129d-e44f-4cb9-8826-85b8426c5640/iso-iec-9594-4-2005>

© ISO/IEC 2005

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 2006

Published in Switzerland

CONTENTS

	<i>Page</i>
1 Scope	1
2 Normative references	1
2.1 Identical Recommendations International Standards	1
2.2 Other references	2
3 Definitions	2
3.1 Communication Model Definitions	2
3.2 Basic Directory Definitions	2
3.3 Directory Model Definitions	2
3.4 DSA Information Model definitions	2
3.5 Abstract Service definitions	3
3.6 Directory replication definitions	3
3.7 Distributed operation definitions	3
4 Abbreviations	5
5 Conventions	5
6 Overview	6
7 Distributed Directory System Model	7
8 DSA Interactions Model	7
8.1 Decomposition of a request	8
8.1.1 NSSR decomposition	8
8.1.2 Request decomposition	8
8.2 Uni-chaining	8
8.3 Multi-chaining	9
8.3.1 Parallel multi-chaining	9
8.3.2 Sequential multi-chaining	9
8.4 Referral	10
8.5 Mode determination	10
9 Overview of DSA Abstract Service	11
10 Information types	11
10.1 Introduction	11
10.2 Information types defined elsewhere	11
10.3 Chaining Arguments	12
10.4 Chaining Results	15
10.5 Operation Progress	15
10.6 Trace Information	16
10.7 Reference Type	16
10.8 Access point information	16
10.9 DIT Bridge knowledge	17
10.10 Exclusions	17
10.11 Continuation Reference	18
11 Bind and Unbind	19
11.1 DSA Bind	19
11.2 DSA Unbind	20
12 Chained operations	20
12.1 Chained operations	20
12.2 Chained Abandon operation	21
12.3 Chained operations and protocol version	21
13 Chained errors	21
13.1 Introduction	21
13.2 DSA Referral	21
14 Introduction	23
14.1 Scope and Limits	23

	<i>Page</i>	
14.2	Conformance.....	23
14.2.1	Interaction involving a first edition DSA.....	23
14.3	Conceptual model	23
14.4	Individual and cooperative operation of DSAs	23
14.5	Cooperative agreements between DSAs.....	24
15	Distributed Directory behaviour	24
15.1	Cooperative fulfilment of operations.....	24
15.2	Phases of operation processing.....	24
15.2.1	Name Resolution phase	24
15.2.2	Evaluation phase	25
15.2.3	Results Merging phase	25
15.3	Managing Distributed Operations.....	25
15.3.1	Request decomposition.....	25
15.3.2	DSA as Request Responder.....	25
15.3.3	Completion of Operations	26
15.4	Loop handling	26
15.4.1	Loop detection.....	26
15.4.2	Loop avoidance.....	26
15.5	Other considerations for distributed operation.....	26
15.5.1	Service controls	26
15.5.2	Extensions	27
15.5.3	Alias dereferencing.....	27
15.5.4	Resolving context-variant names	27
15.5.5	Paged results	27
15.6	Authentication of Distributed Operations.....	28
16	The Operation Dispatcher.....	28
16.1	General Concepts.....	28
16.1.1	Procedures	28
16.1.2	Use of common data structures	28
16.1.3	Errors.....	30
16.1.4	Asynchronous events.....	30
16.2	Procedures of the Operation Dispatcher.....	32
16.3	Overview of procedures.....	33
16.3.1	Request Validation procedure	33
16.3.2	Abandon procedure.....	33
16.3.3	Find DSE procedure	33
16.3.4	Single entry interrogation procedure	34
16.3.5	Modification procedures	34
16.3.6	Multiple entry interrogation procedures	34
16.3.7	Name Resolution Continuation Reference procedure.....	34
16.3.8	List and Search Continuation Reference procedure	34
16.3.9	Result Merging procedure.....	34
17	Request Validation procedure	34
17.1	Introduction	34
17.2	Procedure parameters.....	35
17.2.1	Arguments	35
17.2.2	Results	35
17.3	Procedure definition	36
17.3.1	Abandon processing.....	36
17.3.2	Security checks.....	36
17.3.3	Input preparation.....	36
17.3.4	Validity assertion	37
17.3.5	Loop detection.....	37
17.3.6	Unable or unwilling to perform	37
17.3.7	Output processing.....	38
18	Name Resolution procedure.....	38
18.1	Introduction	38
18.2	Find DSE procedure parameters.....	38

	<i>Page</i>
18.2.1 Arguments	38
18.2.2 Results	38
18.2.3 Errors	39
18.2.4 Global variables	39
18.2.5 Local and shared variables	39
18.3 Procedures	39
18.3.1 Find DSE procedure	40
18.3.2 Target Not Found sub-procedure	43
18.3.3 Target Found sub-procedure	45
18.3.4 Check Suitability procedure	46
19 Operation evaluation	49
19.1 Modification procedure	49
19.1.1 Add Entry Operation	49
19.1.2 Remove Entry Operation	50
19.1.3 Modify Entry Operation	51
19.1.4 Modify DN operation	52
19.1.5 Modify operations and Non-Specific Subordinate References	54
19.2 Single entry interrogation procedure	55
19.3 Multiple entry interrogation procedure	55
19.3.1 List procedures	55
19.3.2 Search procedures	58
20 Continuation Reference procedures	68
20.1 Chaining strategy in the presence of shadowing	68
20.1.1 Master only strategy	70
20.1.2 Parallel strategy	70
20.1.3 Sequential strategy	70
20.2 Issuing chained subrequests to a remote DSA	70
20.3 Procedures' parameters	70
20.3.1 Arguments	70
20.3.2 Results	71
20.3.3 Errors	71
20.4 Definition of the procedures	71
20.4.1 Name Resolution Continuation Reference procedure	71
20.4.2 List Continuation Reference procedure	73
20.4.3 Search Continuation Reference procedure	75
20.4.4 APInfo procedure	76
20.5 Abandon procedure	79
21 Results Merging procedure	80
22 Procedures for distributed authentication	81
22.1 Originator authentication	82
22.1.1 Identity-based authentication	82
22.1.2 Signature-based originator authentication	82
22.2 Results authentication	82
23 Knowledge administration overview	83
23.1 Maintenance of knowledge references	83
23.1.1 Maintenance of consumer knowledge by supplier and master DSAs	83
23.1.2 Maintenance of subordinate and immediate superior knowledge in master DSAs	84
23.1.3 Maintenance of subordinate and immediate superior knowledge in consumer DSAs	84
23.2 Requesting cross reference	84
23.3 Knowledge inconsistencies	85
23.3.1 Detection of knowledge inconsistencies	85
23.3.2 Reporting of knowledge inconsistencies	85
23.3.3 Treatment of inconsistent knowledge references	85
23.4 Knowledge references and contexts	85
24 Hierarchical operational bindings	86
24.1 Operational binding type characteristics	86
24.1.1 Symmetry and roles	86
24.1.2 Agreement	86

	<i>Page</i>
24.1.3 Initiator	86
24.1.4 Establishment parameters.....	87
24.1.5 Modification parameters	88
24.1.6 Termination parameters	88
24.1.7 Type identification	88
24.2 Operational binding information object Class definition.....	88
24.3 DSA procedures for hierarchical operational binding management.....	89
24.3.1 Establishment procedure.....	89
24.3.2 Modification procedure	90
24.3.3 Termination procedure	91
24.4 Procedures for operations	92
24.5 Use of application contexts	92
25 Non-specific hierarchical operational binding.....	92
25.1 Operational binding type characteristics	93
25.1.1 Symmetry and roles	93
25.1.2 Agreement	93
25.1.3 Initiator	93
25.1.4 Establishment parameters.....	93
25.1.5 Modification parameters	94
25.1.6 Termination parameters	94
25.1.7 Type identification	94
25.2 Operational binding information object class definition	94
25.3 DSA procedures for non-specific hierarchical operational binding management	94
25.3.1 Establishment procedure.....	94
25.3.2 Modification procedure	95
25.3.3 Termination procedure	95
25.4 Procedures for operations	96
25.5 Use of application contexts	96
Annex A – ASN.1 for Distributed Operations	97
Annex B – Example of distributed name resolution	101
Annex C – Distributed use of authentication.....	103
C.1 Summary.....	103
C.2 Distributed protection model	103
C.2.1 Quality of protection	103
C.3 Signed chained operations.....	103
C.3.1 Chained signed arguments.....	104
C.3.2 Chained signed results.....	104
C.3.3 Merging of Signed List or Search Results.....	104
C.3.4 Multi-chaining Request	105
C.4 Encrypted chained operations	105
C.4.1 Point-to-point (DUA->DSA or DSA->DSA) encryption on request.....	105
C.4.2 Point-to-point (DUA<-DSA or DSA<-DSA) encryption on result.....	105
C.4.3 End-to-end encryption on DAP Result and point-to-point encryption on DSP Chaining Result	106
C.4.4 Merging of List/Search Results (merging with re-encryption by DSA 1)	106
C.4.5 Merging-not-allowed for List/Search Results	107
C.4.6 Multi-chaining a DAP Request using an Encryption-Key (net-key)	107
C.5 Signed and encrypted distributed operations	108
C.5.1 End-to-end signatures, with point-to-point encryption.....	108
C.5.2 End-to-End Signature and Encryption on DAP Result, Point-to-Point Signature and Encryption on DSP	108
C.5.3 End-to-End Signature on DAP, Point-to-Point Encryption on DSP and DAP Result	109
Annex D – Specification of hierarchical and non-specific hierarchical perational binding types	110
Annex E – Knowledge maintenance example	112
Annex F – Amendments and corrigenda	115

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 9594-4 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.518.

This fifth edition of ISO/IEC 9594-4 constitutes a technical revision of the fourth edition (ISO/IEC 9594-4:2001), which is provisionally retained in order to support implementations based on the fourth edition.

<https://standards.iteh.ai/catalog/standards/sist/834d129d-e44f-4cb9-8826-85b8426e5640/iso-iec-9594-4-2005>

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

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

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

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

This fifth 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 five 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, provides the ASN.1 module for directory distributed operations.

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

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

Annex D, which is an integral part of this Recommendation | International Standard, provides the definitions of the ASN.1 information object classes introduced in this Directory Specification.

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
ITU-T RECOMMENDATION**

**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 the distributed Directory application. The allowed behaviour has been designed so as to ensure a consistent service given a wide distribution of the DIB across many DSAs.

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 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 (2005) | ISO/IEC 9594-1:2005, *Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services.*
- ITU-T Recommendation X.501 (2005) | ISO/IEC 9594-2:2005, *Information technology – Open Systems Interconnection – The Directory: Models.*
- ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*
- ITU-T Recommendation X.511 (2005) | ISO/IEC 9594-3:2005, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition.*
- ITU-T Recommendation X.519 (2005) | ISO/IEC 9594-5:2005, *Information technology – Open Systems Interconnection – The Directory: Protocol specifications.*
- ITU-T Recommendation X.520 (2005) | ISO/IEC 9594-6:2005, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types.*
- ITU-T Recommendation X.521 (2005) | ISO/IEC 9594-7:2005, *Information technology – Open Systems Interconnection – The Directory: Selected object classes.*
- ITU-T Recommendation X.525 (2005) | ISO/IEC 9594-9:2005, *Information technology – Open Systems Interconnection – The Directory: Replication.*
- ITU-T Recommendation X.530 (2005) | ISO/IEC 9594-10:2005, *Information technology – Open Systems Interconnection – The Directory: Use of systems management for administration of the Directory.*
- ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

ISO/IEC 9594-4:2005 (E)

- ITU-T Recommendation X.681 (2002) | ISO/IEC 8824-2:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*
- ITU-T Recommendation X.682 (2002) | ISO/IEC 8824-3:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*
- ITU-T Recommendation X.683 (2002) | ISO/IEC 8824-4:2002, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

2.2 Other references

- IETF RFC 2251 (1997), *Lightweight Directory Access Protocol (v3).*
- IETF RFC 3377 (2002), *Lightweight Directory Access Protocol (v3): Technical Specification.*

3 Definitions

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

3.1 Communication Model Definitions

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

- a) *application-entity-title.*

3.2 Basic Directory Definitions

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

- a) *(the) Directory;*
- b) *Directory Information Base.*

3.3 Directory Model Definitions

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

- a) *access point,*
- b) *alias;*
- c) *distinguished name;*
- d) *Directory Information Tree;*
- e) *Directory System Agent (DSA);*
- f) *Directory User Agent (DUA);*
- g) *relative distinguished name.*

3.4 DSA Information Model definitions

The following terms are defined in ITU-T Rec. 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*.

3.5 Abstract Service definitions

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

- a) *streamed result*.

3.6 Directory replication definitions

The following terms are defined in ITU-T Rec. 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 originator.

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

<https://standards.iteh.ai/catalog/standards/sist/834d129d-e44f-4cb9-8826-85b8426e5646/iso-iec-9594-4-2005>

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 editions prior to the fifth edition.

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 a RHOB regarding DIT vertices superior to the subordinate context prefix.

3.7.6 distributed name resolution: The process by which name resolution is performed in more than one DSA.

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

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

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

3.7.10 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.

3.7.11 initial performer: The first DSA to start performing on an operation, i.e., the first DSA to enter the evaluation phase of the operation.

3.7.12 modification operations: These are the Directory Modify Operations, i.e., Modify Entry, Add Entry, Remove Entry and Modify DN.

3.7.13 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.

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

- 3.7.15 name resolution:** The process of locating an entry by sequentially matching each RDN in a purported name to a vertex of the DIT.
- 3.7.16 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.
- 3.7.17 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.
- 3.7.18 operation progress:** A set of values which denotes the extent to which name resolution has taken place.
- 3.7.19 originator:** The DUA that has initiated a specific (distributed) operation.
- 3.7.20 paging:** A **search** or **list** result is returned piecewise in form of one or more pages that are comprised by a limited number of entries.
- 3.7.21 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.
- 3.7.22 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 14.2 the former variety of input arguments and results are termed external.
- 3.7.23 relevant hierarchical operational binding (RHOB):** Either a HOB or a NHOB, depending on the context.
- 3.7.24 referral:** An outcome which can be returned by a DSA which cannot perform an operation itself, and which identifies one or more other DSAs more able to perform the operation.
- 3.7.25 reply:** A result or an error. (standards.iteh.ai)
- 3.7.26 request:** Information consisting of an operation code and associated arguments to convey a directory operation from a requester to a performer. <https://standards.iteh.ai/catalog/standards/sist/834d129d-e44f-4cb9-8826-808426c30404/iso-9594-4-2005>
- 3.7.27 request decomposition:** Decomposition of a request into subrequests for other DSAs to pursue; these subrequests may be either chained to these DSAs by the DSA performing the decomposition, or continuation references 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.
- 3.7.28 requester:** A DUA or DSA sending a request to perform (i.e., invoke) an operation.
- 3.7.29 single entry interrogation operations:** These are the Directory Read Operations, i.e., Read and Compare.
- 3.7.30 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.
- 3.7.31 subordinate DSA:** Of the two DSAs sharing a HOB or a NHOB, the DSA holding the subordinate naming context.
- 3.7.32 subrequest:** A request generated by request decomposition.
- 3.7.33 superior DSA:** Of the two DSAs sharing a HOB or a NHOB, the DSA holding the superior naming context.
- 3.7.34 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 a HOB (or NHOB), or exists implicitly by virtue of the superior DSA holding a subordinate (or non-specific subordinate) reference to the subordinate DSA.
- 3.7.35 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.
- 3.7.36 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 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
DISP	Directory Information Shadowing Protocol
DMD	Directory Management Domain
DOP	Directory Operational Binding Management Protocol
DSE	DSA-Specific Entry
HOB	Hierarchical Operational Binding
NHOB	Non-specific Hierarchical Operational Binding
NSSR	Non-specific Subordinate Reference
RHOB	Relevant Hierarchical Operational Binding

5 Conventions

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

The term "Directory Specification" (as in "this Directory Specification") shall be taken to mean ITU-T Rec. X.518 | ISO/IEC 9594-4. 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 *first edition systems* to refer to systems conforming to the first edition of the Directory Specifications, i.e., the 1988 edition of the series of CCITT X.500 Recommendations and the ISO/IEC 9594:1990 edition. This Directory Specification uses the term *second edition systems* to refer to systems conforming to the second edition of the Directory Specifications, i.e., the 1993 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:1995 edition. This Directory Specification uses the term *third edition systems* to refer to systems conforming to the third edition of the Directory Specifications, i.e., the 1997 edition of the series of ITU-T X.500 Recommendations and the ISO/IEC 9594:1998 edition. This Directory Specification uses the term *fourth edition systems* to refer to systems conforming to the fourth edition of the Directory Specifications, i.e., the 2001 editions of ITU-T Recs X.500, X.501, X.511, X.518, X.519, X.520, X.521, X.525, and X.530, the 2000 edition of ITU-T Rec. X.509, and parts 1-10 of the ISO/IEC 9594:2001 edition.

This Directory Specification uses the term *fifth edition systems* to refer to systems conforming to the fifth edition of the Directory Specifications, i.e., the 2005 editions of ITU-T Recs X.500, X.501, X.509, X.511, X.518, X.519, X.520, X.521, X.525, and X.530 and parts 1-10 of the ISO/IEC 9594:2005 edition.

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

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 described in terms of the abstract Directory object as specified in ITU-T Rec. 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 RFC 3377.

Necessarily, the specification of the abstract Directory object does not in any way address the physical realization of the Directory: in particular it 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 number of DSAs. Consequently, the requirements for DSAs to have knowledge of, navigate to, and cooperate with other DSAs, in order to support the abstract service in a distributed environment is also not covered by the service description.

This Directory Specification specifies the refinement of the abstract Directory object, the refinement being expressed in terms of a set of one or more DSA objects which 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. 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 DSA(s), has the option of interrogating the other DSA(s) directly (chaining) or, whether it should respond with information about other DSA(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.

SECTION 3 – DISTRIBUTED DIRECTORY MODELS

7 Distributed Directory System Model

The Directory abstract service, as defined in ITU-T Rec. X.511 | ISO/IEC 9594-3, models the Directory as an object which provides a set of directory services to its users. Users of the Directory access its services through an access point. The Directory may have one or more access points and each access point is characterized by the services it provides and the mode of interaction used to provide these services.

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.

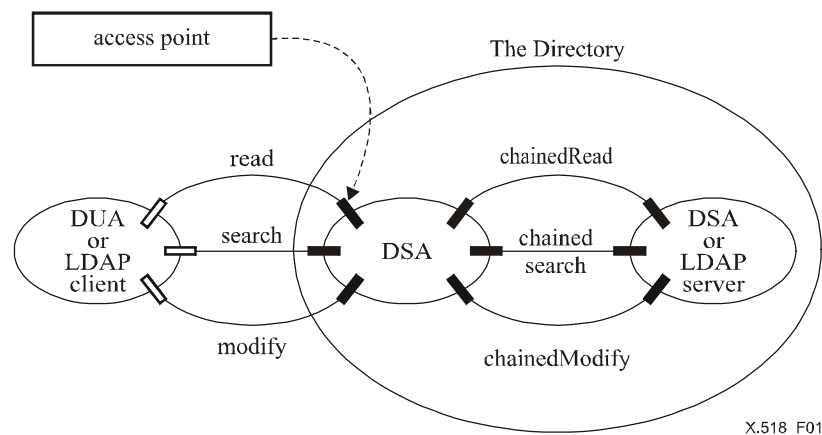


Figure 1 – Objects of the distributed Directory model
(standards.iteh.ai)

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 can interact in a prescribed, cooperative manner to provide directory services to the users of the directory (DUAs or LDAP clients).

Figure 1 illustrates the relationship between the Directory abstract service and the DSA abstract service. The Directory abstract service defined in ITU-T Rec. X.511 | ISO/IEC 9594-3 is provided through a number of Directory operations. To realize this service, the DSAs 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. 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.

NOTE – It may also be possible for DSAs that are LDAP requestors to chain operations, for example, using LDAP Controls or Extended Operations; however, the procedures and protocols necessary to achieve this are outside the scope of this Directory Specification.

8 DSA Interactions Model

A basic characteristic of the Directory is that, given a distributed DIB, a user should potentially be able to have any service request satisfied (subject to security, access control, and administrative policies) irrespective of the access point at which the request originates. In accommodating this requirement, it is necessary that any DSA involved in satisfying a particular service request have some knowledge (as specified in ITU-T Rec. X.501 | ISO/IEC 9594-2) of where the requested information is located and either return this knowledge to the requester or attempt to have the request satisfied on its behalf. (The requester may be a DUA, an LDAP client or another DSA: in the latter case both DSAs shall support the DSP.)

Three modes of DSA interaction are defined to meet these requirements, namely "uni-chaining", "multi-chaining", and "referral". Throughout the remainder of this Directory Specification, the generic term chaining is used to refer to uni-