

/ Draft Technical Standard

Server Profiles of the Lightweight Directory Access Protocol (LDAP)

Draft 1.0

The Open Group



© *September 1998, The Open Group*

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the copyright owners.

© *1997-1998 Innosoft International*

Chapters 1-4 of this document are derived from the January 6 1988 Draft LDAP Server Profiles of Critical Angle Inc., copyright © 1997-1998 by Critical Angle Inc. Critical Angle's rights in that material are now owned by Innosoft International, Inc., 1050 Lakes Drive, West Covina, CA 91790-2923, USA.

Draft Technical Standard

Server Profiles of the Lightweight Directory Access Protocol (LDAP) Draft 1.0

ISBN: ?-?????-???-?

Document Number: C???

Published in the U.K. by The Open Group, September 1998.

Any comments relating to the material contained in this document may be submitted to:

The Open Group
Apex Plaza
Forbury Road
Reading
Berkshire, RG1 1AX
United Kingdom

or by Electronic Mail to:

OGSpecs@opengroup.org

Contents

Chapter 1	Read-Only LDAP Server Profile	1
1.1	Introduction.....	1
1.2	References	1
1.3	General Requirements.....	2
1.4	Network Requirements.....	2
1.5	Directory Information Tree Requirements.....	2
1.6	Directory Attribute Model Requirements.....	3
1.6.1	Root DSE Requirements.....	3
1.6.2	Entry Requirements	3
1.6.3	Subschema Entry Requirements	3
1.7	Distinguished Name Requirements	4
1.8	General Request Processing Requirements	4
1.9	Bind Request Processing Requirements	5
1.10	Search Request Processing Requirements.....	5
1.10.1	Search Filter Processing Requirements.....	5
1.10.2	Additional Requirements for Operations Based at a Context Prefix	7
1.11	Compare Request Processing Requirements.....	7
1.12	Requirements for Processing DIT Modification Requests	8
Chapter 2	Read-Write LDAP Server Profile	9
2.1	Introduction.....	9
2.2	References	9
2.3	General Requirements.....	10
2.4	Directory Information Tree Requirements.....	10
2.5	Directory Attribute Model Requirements.....	11
2.5.1	Root DSE Requirements.....	11
2.5.2	Entry Requirements	11
2.5.3	Subschema Entry Requirements	12
2.5.4	Referral DSE Requirements.....	12
2.6	General Request Processing Requirements	12
2.7	Bind Request Processing Requirements	12
2.8	Add Request Processing Requirements.....	13
2.9	Modify Request Processing Requirements	13
2.10	Delete Request Processing Requirements.....	14
2.11	Modify DN Request Processing Requirements.....	14
2.12	Protocol Security Requirements.....	14
Chapter 3	White Pages Application LDAP Server Profile.....	15
3.1	Introduction.....	15
3.2	References	15
3.3	General Requirements.....	16
3.4	Schema Requirements	16

Chapter 4	Certificate Application LDAP Server Profile	19
4.1	Introduction.....	19
4.2	References	19
4.3	General Requirements.....	19
4.4	Schema Requirements	20
4.5	Attributes Requiring Special Handling	21
4.6	Bind Operation Requirements.....	21
Chapter 5	The ogSupportedProfile Attribute.....	23
Appendix A	Object Identifier Assignment.....	25
Appendix B	The Lightweight Internet Person Schema (LIPS).....	27
	Glossary	29
	Index	33
 List of Tables		
1-1	Selected String-based Syntaxes.....	5
1-2	White space characters	6
2-1	Selected Syntaxes with which the Binary Option can be Used.....	11



Preface

The Open Group

The Open Group is the leading vendor-neutral, international consortium for buyers and suppliers of technology. Its mission is to cause the development of a viable global information infrastructure that is ubiquitous, trusted, reliable, and as easy-to-use as the telephone. The essential functionality embedded in this infrastructure is what we term the *IT DialTone*. The Open Group creates an environment where all elements involved in technology development can cooperate to deliver less costly and more flexible IT solutions.

Formed in 1996 by the merger of the X/Open Company Ltd. (founded in 1984) and the Open Software Foundation (founded in 1988), The Open Group is supported by most of the world's largest user organizations, information systems vendors, and software suppliers. By combining the strengths of open systems specifications and a proven branding scheme with collaborative technology development and advanced research, The Open Group is well positioned to meet its new mission, as well as to assist user organizations, vendors, and suppliers in the development and implementation of products supporting the adoption and proliferation of systems which conform to standard specifications.

With more than 200 member companies, The Open Group helps the IT industry to advance technologically while managing the change caused by innovation. It does this by:

- Consolidating, prioritizing, and communicating customer requirements to vendors
- Conducting research and development with industry, academia, and government agencies to deliver innovation and economy through projects associated with its Research Institute
- Managing cost-effective development efforts that accelerate consistent multi-vendor deployment of technology in response to customer requirements
- Adopting, integrating, and publishing industry standard specifications that provide an essential set of blueprints for building open information systems and integrating new technology as it becomes available
- Licensing and promoting the Open Brand, represented by the "X" Device, that designates vendor products which conform to Open Group Product Standards
- Promoting the benefits of the IT DialTone to customers, vendors, and the public

The Open Group operates in all phases of the open systems technology lifecycle including innovation, market adoption, product development, and proliferation. Presently, it focuses on seven strategic areas: open systems application platform development, architecture, distributed systems management, interoperability, distributed computing environment, security, and the information superhighway. The Open Group is also responsible for the management of the UNIX trademark on behalf of the industry.

Development of Product Standards

This process includes the identification of requirements for open systems and, now, the IT DialTone, development of Technical Standards (formerly CAE and Preliminary Specifications) through an industry consensus review and adoption procedure (in parallel with formal standards work), and the development of tests and conformance criteria.

This leads to the preparation of a Product Standard which is the name used for the documentation that records the conformance requirements (and other information) to which a vendor may register a product.

The “X” Device is used by vendors to demonstrate that their products conform to the relevant Product Standard. By use of the Open Brand they guarantee, through the Open Brand Trade Mark License Agreement (TMLA), to maintain their products in conformance with the Product Standard so that the product works, will continue to work, and that any problems will be fixed by the vendor.

Open Group Publications

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical Standards and product documentation, but which also includes Guides, Snapshots, Technical Studies, Branding and Testing documentation, industry surveys, and business titles.

There are several types of specification:

- *Technical Standards* (formerly *CAE Specifications*)

The Open Group Technical Standards form the basis for our Product Standards. These Standards are intended to be used widely within the industry for product development and procurement purposes.

Anyone developing products that implement a Technical Standard can enjoy the benefits of a single, widely supported industry standard. Where appropriate, they can demonstrate product compliance through the Open Brand. Technical Standards are published as soon as they are developed, so enabling vendors to proceed with development of conformant products without delay.

- *CAE Specifications*

CAE Specifications and Developers' Specifications published prior to January 1998 have the same status as Technical Standards (see above).

- *Preliminary Specifications*

Preliminary Specifications have usually addressed an emerging area of technology and consequently are not yet supported by multiple sources of stable conformant implementations. They are published for the purpose of validation through implementation of products. A Preliminary Specification is as stable as can be achieved, through applying The Open Group's rigorous development and review procedures.

Preliminary Specifications are analogous to the *trial-use* standards issued by formal standards organizations, and developers are encouraged to develop products on the basis of them. However, experience through implementation work may result in significant (possibly upwardly incompatible) changes before its progression to becoming a Technical Standard. While the intent is to progress Preliminary Specifications to corresponding Technical Standards, the ability to do so depends on consensus among Open Group members.

- *Consortium and Technology Specifications*

The Open Group publishes specifications on behalf of industry consortia. For example, it publishes the NMF SPIRIT procurement specifications on behalf of the Network Management Forum. It also publishes Technology Specifications relating to OSF/1, DCE, OSF/Motif, and CDE.

Technology Specifications (formerly AES Specifications) are often candidates for consensus review, and may be adopted as Technical Standards, in which case the relevant Technology Specification is superseded by a Technical Standard.

In addition, The Open Group publishes:

- *Product Documentation*

This includes product documentation—programmer's guides, user manuals, and so on—relating to the Pre-structured Technology Projects (PSTs), such as DCE and CDE. It also includes the Single UNIX Documentation, designed for use as common product documentation for the whole industry.

- *Guides*

These provide information that is useful in the evaluation, procurement, development, or management of open systems, particularly those that relate to the Technical Standards or Preliminary Specifications. The Open Group Guides are advisory, not normative, and should not be referenced for purposes of specifying or claiming conformance to a Product Standard.

- *Technical Studies*

Technical Studies present results of analyses performed on subjects of interest in areas relevant to The Open Group's Technical Program. They are intended to communicate the findings to the outside world so as to stimulate discussion and activity in other bodies and the industry in general.

Versions and Issues of Specifications

As with all *live* documents, Technical Standards and Specifications require revision to align with new developments and associated international standards. To distinguish between revised specifications which are fully backwards compatible and those which are not:

- A new *Version* indicates there is no change to the definitive information contained in the previous publication of that title, but additions/extensions are included. As such, it *replaces* the previous publication.
- A new *Issue* indicates there is substantive change to the definitive information contained in the previous publication of that title, and there may also be additions/extensions. As such, both previous and new documents are maintained as current publications.

Corrigenda

Readers should note that Corrigenda may apply to any publication. Corrigenda information is published on the World-Wide Web at <http://www.opengroup.org/corrigenda>.

Ordering Information

Full catalogue and ordering information on all Open Group publications is available on the World-Wide Web at <http://www.opengroup.org/pubs>.

This Document

This document is a Draft Technical Standard consisting of a set of profiles of the Lightweight Directory Access Protocol (LDAP) and related standards to which Directory Servers can conform. The standards on which it is based are mainly Requests for Comment (RFCs) of the Internet Engineering Task Force (IETF).

Structure

- Chapter 1 defines the Read-Only Server Profile. Servers that perform read operations can conform to this profile without having to support write operations.
- Chapter 2 defines the Read/Write Server Profile. Servers that conform to this profile support the full range of LDAP operations.
- Chapter 3 defines the Internet White Pages Server Application Profile, designed for use by applications that provide a “white pages” directory service for Internet users.
- Chapter 4 defines the Certificates Server Application Profile, designed for use in the certificate storage and retrieval application.
- Chapter 5 defines the **ogSupportedProfile** attribute. This attribute indicates which profiles a server supports.
- Appendix A describes how object identifiers (OIDs) are allocated to the **ogSupportedProfile** attribute and its values.
- Appendix B contains a version of the NAC LIPS schema.
- The Glossary expands abbreviations used in this document and gives brief explanations of frequently used technical terms.

Terminology

The following terms are used in this specification with the following meanings when applied to client or server behavior.

can

This describes a permissible optional behavior. Servers must allow for, but should not rely on, such behavior in clients, and vice versa.

may

This means that the feature or behavior is optional. Clients should not rely on the behavior in servers, and vice versa. To avoid ambiguity, the reverse sense of *may* is expressed as *need not*, instead of *may not*.

must

This describes a requirement on the client or server.

need not

This is the opposite of *may*.

shall

This is equivalent to *must*.

should

This means that the behavior is recommended, but is not mandatory. Clients should not rely on the behavior in servers, and vice versa.

Preface

will

This is equivalent to *must*.

Typographical Conventions

The following typographical conventions are used throughout this document:

- **Bold** font is used in text for
 - directory object classes and attributes
 - LDAP data units and fields.
- *Italic* font is used
 - for attribute values
 - for emphasis
 - to identify the first instance of a word requiring definition.
- Fixed width font is used for
 - directory syntaxes
 - formal definitions of object classes and attributes.

Change History

- **Issue 1 Draft 1.0:**
This is the first issue of this document.

Acknowledgements

The base documents for this specification were produced by Mark Wahl of Critical Angle Inc. The Open Group gratefully acknowledges this contribution and thanks Innosoft International Inc., the current owner of the copyright in the base documents, for their permission for the work to be incorporated in this publication.

The Open Group thanks the Network Applications Consortium for their kind permission to reproduce the version of LIPS in Appendix B on page 27.

Finally, the Open Group thanks the members of the LDAP Profile Specification Working Group for their contribution to the development of this specification. They are listed below, along with their corporate affiliation at the time of their contribution.

Chris Apple	AT&T
Clive Betteridge	Eurosinet
Robert Early	Isocor
Patrick Fantou	SNI
David Finkelstein	Xcert
Tim Howes	Netscape
Satoshi Kikuchi	Hitachi
William King	Mount Bonnell
Greg Lavender	Critical Angle
Declan McMahon	Isocor
Ludovic Poitou	Sun
Bero Porter	GTE
Patrick Richard	Xcert
Tatsuji Shimoe	Fujitsu
Ellen Stokes	IBM
Mark Wahl	Critical Angle
Chris Weider	Microsoft
Russel Weiser	Novell

Trade Marks

Motif[®], OSF/1[®], UNIX[®], and the “X Device”[®] are registered trademarks and IT DialTone[™] and The Open Group[™] are trademarks of The Open Group in the U.S. and other countries.

Referenced Documents

Primary References

The following documents are referenced in the body of this specification:

ISO 8859

ISO/IEC 8859-1:1998 Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1 and Part 2: Latin alphabet No. 2.¹

ISO 10646

ISO/IEC 10646-1:1993. Information technology — Universal Multiple-Octet Coded Character Set (UCS) — Part 1: Architecture and Basic Multilingual Plane.

LDAP Authentication

Internet Draft draft-ietf-ldapext-authmeth-01. The latest version is draft-ietf-ldapext-authmeth-02 — Authentication Methods for LDAP. M. Wahl, H. Alvestrand, J.Hodges, R.Morgan. July 1998.²

LDAP over TLS

Internet Draft draft-ietf-asis-ldapv3-tls-02 — Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security. J.hodges, R.Morgan, M.wahl. August 1998.³

PKIX LDAPv2

Internet Draft draft-ietf-pkix-ipki2opp-07 — Internet X.509 Public Key Infrastructure Operational Protocols — LDAPv2. S. Boeyen, T.Howes, P.Richard. March 1998.⁴

Referrals

Internet Draft draft-ietf-ldapext-referral-00 — Referrals and Knowledge References in LDAP Directories. M.Wahl, T.Howes. March 1998.⁵

RFC 791

IETF RFC 791: Internet Protocol. J. Postel. September 1981.⁶

RFC 793

IETF RFC 793: Transmission Control Protocol. J. Postel. September 1981.

RFC 1274 IETF RFC 1274: The COSINE and Internet X.500 Schema. P. Barker, S. Kille. November 1991.

RFC 1777 IETF RFC 1777: Lightweight Directory Access Protocol. W. Yeong, T. Howes & S. Kille. March 1995.

-
1. Information about the International Organization for Standardization (ISO) and International Standards is available from the ISO Web Site at <http://www.iso.ch>.
 2. This draft expires in January 1999. Until then it is available from <http://www.ietf.org/internet-drafts/draft-ietf-ldapext-authmeth-02.txt>.
 3. This draft expires in February 1999. Until then it is available from <http://www.ietf.org/internet-drafts/draft-ietf-ldapext-ldapv3-tls-02.txt>.
 4. This draft expires in September 1998. Until then it is available from <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki2opp-07.txt>.
 5. This draft expires in September 1998. Until then it is available from <http://www.ietf.org/internet-drafts/draft-ietf-ldapext-referral-00.txt>.
 6. IETF RFCs are available online from the IETF Web Site at <http://www.ietf.org/>.

Referenced Documents

RFC 2079

IETF RFC 2079: Definition of an X.500 Attribute Type and an Object Class to Hold Uniform Resource Identifiers (URIs). M. Smith. January 1997.

RFC 2195

IETF RFC 2195: IMAP/POP AUTHorize Extension for Simple Challenge/Response. J. Klensin, R. Catoe, P. Krumviede. September 1997.

RFC 2222 IETF RFC 2222: Simple Authentication and Security Layer (SASL). J. Myers. October 1997.

RFC 2251

IETF RFC 2251: Lightweight Directory Access Protocol (v3). M. Wahl, T. Howes, S. Kille. December 1997.

RFC 2252

IETF RFC 2252: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions. M. Wahl, A. Coulbeck, T. Howes, S. Kille. December 1997.

RFC 2253

IETF RFC 2253: Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names. M. Wahl, S. Kille, T. Howes. December 1997.

RFC 2254

IETF RFC 2254: The String Representation of LDAP Search Filters. T. Howes. December 1997.

RFC 2255

IETF RFC 2255: The LDAP URL Format. T. Howes, M. Smith. December 1997.

RFC 2256

IETF RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3. M. Wahl.

UNICODE

The Unicode Standard, Version 2.0. Published by Addison Wesley, 1996 ISBN 0-201-48345-9.⁷

Informational References

The following documents are referenced in the Glossary.

ISO 8824

ISO/IEC 8824: 1990, Information Technology — Open Systems Interconnection — Specification of Abstract Syntax Notation 1 (ASN.1).

SSL

A. Frier, P. Karlton, and P. Kocher: The SSL 3.0 Protocol, Netscape Communications Corporation, November 1996.⁸

T.61

ITU-T (formerly CCITT) Recommendation T.61 — Character Repertoire and Coded Character Sets for the International Teletex Service.⁹

7. Information about Unicode is available from the Unicode Consortium Web Site at <http://www.unicode.org>.

8. Information about Netscape is available from their Web Site at <http://www.netscape.com>.

9. Information about the International Telecommunications Union (ITU), and its Telecommunication Standardization Sector (ITU-T), and ITU-T Recommendations is available from the ITU Web Site at <http://www.itu.ch>.

TLS

Internet Draft draft-ietf-tls-protocol-05 — The TLS Protocol Version 1.0. T.Dierks, C.Allen. November 1997.¹⁰

X.500

ITU-T (formerly CCITT) Recommendation X.500 and other recommendations in the X.500 series, and ISO/IEC 9594 (the parts of which are technically aligned with the X.500 series recommendations): Information Technology — Open Systems Interconnection — The Directory.

10. This draft has already expired, but may be available from <http://www.ietf.org/internet-drafts/draft-ietf-tls-protocol-05.txt>.

Read-Only LDAP Server Profile

1

1.1 Introduction

2

This chapter defines a functional subset of the LDAP protocol definitions to be implemented by LDAP server products. This subset is designed for use by applications that require read access to information held in the directory.

3

Note: Some of the base documents on which this profile is based are currently at Internet Draft status. The reader is warned that the material in these drafts is subject to change. This profile will be updated to reference the RFCs that result from these drafts once they are approved by the IETF.

4

1.2 References

5

This functional subset of LDAP is defined by the following IETF specifications.

6

RFC 1777

7

RFC 2251

8

RFC 2252

9

RFC 2253

10

RFC 2254

11

RFC 2255

12

RFC 2256

13

All statements in these documents listed as “MUST” requirements for a server, with the exception of statements related exclusively to the Add, Delete, Modify and Modify DN operations, shall be implemented.

14

The following documents are also referenced by this profile:

15

the **UNICODE** Standard

16

ISO 10646

17

RFC 793

18

RFC 791

19

the **Referrals** Internet Draft

20

ISO 8859

21

The **ogSupportedProfile** attribute referred to in this profile is defined in Chapter 5 on page 23.

22

1.3	General Requirements	23
	The phrase <i>RO LDAP server</i> used in this document refers to a product that conforms to this <i>read-only</i> functional subset.	24
	A RO LDAP server is defined as a network entity that accepts connections and responds to requests formatted according to the Lightweight Directory Access Protocol made on those connections. The RO LDAP server processes the requests in accordance with the semantics associated with the LDAP operations.	25
	If the entity responding to LDAP requests translates these requests into another protocol, such as the X.500 Directory Access Protocol (DAP), for processing by another network entity, then the RO LDAP server is defined to be the combination of the LDAP translator and all other network-accessible entities that are involved in processing requests.	26
1.4	Network Requirements	27
	A RO LDAP server shall accept connections in the Transport Control Protocol (TCP) (defined by RFC 793) carried over Internet Protocol (IP) version 4 (defined by RFC 791). Future versions of this profile may specify in addition the use of IP version 6.	28
	By default a RO LDAP server shall accept connections on TCP port 389, which has been assigned by the Internet Assigned Numbers Authority (IANA). A RO LDAP server shall support multiple simultaneous connections.	29
1.5	Directory Information Tree Requirements	30
	A directory information tree is partitioned into one or more naming contexts, each a contiguous subtree of entries. A RO LDAP server shall hold at least one naming context.	31
	Every directory entry must be identifiable by its name. A RO LDAP server shall support client searches in which the base object of the search request is any entry in any naming context held by the server, and any of the three search scopes are specified, without returning a result indicating a naming error.	32
	If a RO LDAP server can be configured to hold a naming context whose context prefix is not immediately subordinate to the root, then the server shall support the return of referrals for superior references as defined in the Referrals Internet Draft.	33
	If a RO LDAP server holds a naming context (B) and can be configured to have knowledge of one or several naming contexts subordinate to (B) then the server shall support the return of referrals for subordinate references and the return of search continuation references as defined in the Referrals Internet Draft.	34
	A RO LDAP server shall hold the root DSA-Specific Entry (DSE). The root DSE is not part of any naming context.	35
	A RO LDAP server shall be capable of holding at least one subschema entry.	36
	A RO LDAP server is not required to implement aliases.	37

1.6	Directory Attribute Model Requirements	38
	The ability for the client to retrieve values of attributes in DSEs and entries described in the following subsections may be restricted by access control.	39
1.6.1	Root DSE Requirements	40
	A RO LDAP server shall provide the following attributes in the root DSE: namingContexts , subschemaSubentry , ogSupportedProfile and supportedLDAPVersion . Return of values containing Distinguished Names may be subject to access control restrictions.	41
	A RO LDAP server shall provide a value of the namingContexts attribute for each naming context held by the server. However, if all naming contexts held by the server are immediately subordinate to the root DSE, and the server does not support the return of referrals for subordinate references or the return of search continuation references, then the server shall instead provide only one value of the namingContexts attribute, a string of zero length.	42
	A RO LDAP server shall provide a value of the subschemaSubentry attribute for each subschema entry held by the server.	43
	A RO LDAP server shall provide the value 1.2.826.0.1050.11.1.1 in the ogSupportedProfile attribute.	44
	A RO LDAP server shall provide the values 2 and 3 in the supportedLDAPVersion attribute.	45
1.6.2	Entry Requirements	46
	A RO LDAP server shall always support the following attributes in each entry: objectClass and subschemaSubentry . Return of values may be subject to access control restrictions.	47
	The objectClass attribute in an entry shall always have at least one of these two values: <i>top</i> or <i>alias</i> . An additional value will be present for each other object class of the entry.	48
	The subschemaSubentry attribute in an entry has exactly one value.	49
1.6.3	Subschema Entry Requirements	50
	A RO LDAP server shall provide in each subschema entry the attributes listed in section 3.2.2 of RFC 2251 .	51
	The objectClasses attribute shall contain values for the object classes top and subschema . The SUP , MUST and MAY fields in these ObjectClassDescription values shall match the definitions in RFC 2252 . Additional values of the objectClasses attribute can be present.	52
	The attributeTypes attribute shall contain values for the attribute types objectClass and subschemaSubentry and all attribute types which are present in the root DSE and the subschema entries. The SUP and SYNTAX fields in these AttributeTypeDescription values shall match the definitions in RFC 2252 . Additional values of the attributeTypes attribute may be present.	53
	A RO LDAP server that supports the return of referrals may allow its administrator to configure that subschema entries are held in another server. In this case, the server may also provide values of the subschemaSubentry attribute in the root DSE and in entries in which the named subschema entry is not held by that server.	54

1.7	Distinguished Name Requirements	55
	A RO LDAP server shall support all forms of quoting described in RFC 2253 for LDAPDN fields and attribute values received in requests.	56
	A RO LDAP server that supports entries with multi-valued Relative Distinguished Names (RDNs) shall ignore differences in the order in which Attribute Value Assertion (AVA) components occur when comparing Distinguished Names (DNs) for equality.	57
	A RO LDAP server shall compare Distinguished Names according to equality matching rules defined for the attributes in each component.	* 58
1.8	General Request Processing Requirements	59
	A RO LDAP server shall support client requests of 64K bytes in size (measured as the sum of the sizes of the TCP packets containing the request, excluding the TCP and lower-level protocol headers).	60
	A RO LDAP server shall reject requests that contain controls marked critical when the controlType field is not recognized.	61
	A RO LDAP server shall permit search, compare, abandon and unbind operations to be performed without requiring them to be preceded by a bind operation.	62
	A RO LDAP server shall permit the client to perform the bind operation multiple times on a connection.	63
	If a RO LDAP server supports the return of referrals, and a client that has bound indicating protocol version 2 submits a request for which the server would in the LDAPv3 situation return a referral, the server shall behave as an LDAPv2 server performing the same operation.	64
	If a RO LDAP server supports the return of search continuation references, and a client which has bound indicating protocol version 2 submits a request for which the server would in the LDAPv3 situation return one or more search continuation references followed by resultCode 0 , the server shall not return any search continuation references. Instead, it shall behave as an LDAPv2 server and send only the searchResultEntry corresponding to the entries held locally.	65
	A RO LDAP server shall not close the connection unless it has received an UnbindRequest from the client, returned a notice of disconnection to the client, or the client has been idle (no requests have been processed) for thirty minutes. A RO LDAP server need not implement the closing of idle connections.	66
	A RO LDAP server shall return the protocolError for requests of an unparseable form, and for ExtendedRequest with an unrecognized OID.	67
	If a client has bound to a RO LDAP server indicating protocol version 2, then the RO LDAP server must not send UTF-8 encodings for characters other than US-ASCII characters, but must send the corresponding T.61 encodings.	68

1.9	Bind Request Processing Requirements	69
	A RO LDAP server shall accept the BindRequest in which the version field is 2 or 3, the name field is of zero length, the authentication choice is simple, and the simple field is of zero length, and return the resultCode 0 .	70
	A RO LDAP server shall return the resultCode authMethodNotSupported if the authentication choice is <i>sasl</i> and the SASL mechanism is not supported.	71
	A RO LDAP server need not implement any SASL mechanisms. ¹	72
	A RO LDAP server shall reject a bind request if it contains a Distinguished Name with attribute types that the server does not recognize.	73
1.10	Search Request Processing Requirements	74
	A RO LDAP server shall recognize the attribute type "*" in the attributes field list.	75
	A RO LDAP server shall not return an error if the attributes field contains unrecognized attribute types or unrecognized attribute description options.	76
	A RO LDAP server may contain an internally-defined upper limit on the number of entries that can be returned. This limit, if present, shall be configurable by the administrator.	77
	If a request contains a DN with attribute types that the server does not recognize:	78
	• if the request holds a superior reference then a RO LDAP server shall return a superior reference	79
	• otherwise, a RO LDAP server shall return resultCode 32, noSuchObject .	80
1.10.1	Search Filter Processing Requirements	81
	A RO LDAP server shall implement search filtering as described in section 4.5.1 of RFC 2251 . A RO LDAP server shall be capable of handling search filters containing unrecognized attribute types.	82
	A RO LDAP server shall be capable of performing searches specifying greaterOrEqual and lessOrEqual filters on values of the createTimestamp and modifyTimestamp attribute types.	83

1. unless it is also a RW LDAP server, see Section 2.7 on page 12

Syntax	OID
Country String	1.3.6.1.4.1.1466.115.121.1.11
Directory String	1.3.6.1.4.1.1466.115.121.1.15
Numeric String	1.3.6.1.4.1.1466.115.121.1.36
Postal Address	1.3.6.1.4.1.1466.115.121.1.41
Printable String	1.3.6.1.4.1.1466.115.121.1.44
Telephone Number	1.3.6.1.4.1.1466.115.121.1.50

*

Table 1-1 Selected String-based Syntaxes

Unless indicated otherwise by the matching rule definition, equality, substring and approximate match search filters involving attribute types with syntaxes from Table 1-1 shall ignore the case of letters of the Latin alphabets 1 and 2 defined in **ISO 8859** when performing the comparison. In addition, leading and trailing whitespace characters in the assertion and attribute values are to be ignored, multiple adjoining whitespace characters are to be treated as a single whitespace character, and any two whitespace characters compare as equal.

Table 1-2 lists the whitespace characters, defined by part 1 clause 21 of **ISO 10646**.

Character Name	Unicode Value	UTF-8 Value
HORIZONTAL TABULATION	0009	09
LINE FEED	000A	0A
VERTICAL TABULATION	000B	0B
FORM FEED	000C	0C
CARRIAGE RETURN	000D	0D
SPACE	0020	20
NO-BREAK SPACE	00A0	C2 80
EN QUAD	2000	E2 80 80
EM QUAD	2001	E2 80 81
EN SPACE	2002	E2 80 82
EM SPACE	2003	E2 80 83
THREE-PER-EM SPACE	2004	E2 80 84
FOUR-PER-EM SPACE	2005	E2 80 85
SIX-PER-EM SPACE	2006	E2 80 86
FIGURE SPACE	2007	E2 80 87
PUNCTUATION SPACE	2008	E2 80 88
THIN SPACE	2009	E2 80 89
HAIR SPACE	200A	E2 80 8A
IDEOGRAPHIC SPACE	3000	E3 80 80
ZERO WIDTH NO-BREAK SPACE	FEFF	EF BB BF

Table 1-2 White space characters

Unless indicated otherwise by the matching rule definition, RO LDAP servers shall accept in assertion values used in comparison with attributes having the `Directory String` syntax (1.3.6.1.4.1.1466.115.121.1.15) the UTF-8 encoding of any character from the **UNICODE** Standard.

A RO LDAP server may evaluate to <i>Undefined</i> a match by a client that has bound indicating protocol version 2 when the attribute has a syntax listed in Table 1-1 on page 6 and the assertion value contains one or more non-ASCII characters.	91
Unless indicated otherwise by the matching rule definition, RO LDAP servers need not be able to recognize equivalent sequences in attributes having the Directory String syntax in which static precomposed and dynamically composed characters are being compared, or compatibility characters and non-compatibility characters are being compared.	92
A RO LDAP server shall ensure that when an equality matching rule for an attribute evaluates to <i>TRUE</i> with a particular attribute value and assertion value, the approximate matching rule for the attribute, if it has been defined, also evaluates to <i>TRUE</i> , and the ordering matching rule, if it has been defined, evaluates to <i>FALSE</i> .	93
A RO LDAP server that supports extensibleMatch functionality shall behave as follows.	94
<ul style="list-style-type: none"> • It shall ensure that the evaluation of an extensibleMatch in which the matchingRule field is absent, the type field is present, and the dnAttributes field is <i>FALSE</i> is identical to an equalityMatch filter with the same attribute type and assertion value. 	95
<ul style="list-style-type: none"> • If it supports at least one matching rule then it shall be capable of performing an extensibleMatch in which the matchingRule field is one supported by the server and the type field is absent. 	96
<ul style="list-style-type: none"> • It shall be capable of performing an extensibleMatch in which the dnAttributes field is <i>TRUE</i>. 	97
A RO LDAP server that does not support extensibleMatch functionality shall return resultCode 12 when a client submits a request containing an extensibleMatch .	98
1.10.2 Additional Requirements for Operations Based at a Context Prefix	99
This section describes the behavior of a RO LDAP server for a search request in which the baseObject field is the context prefix of a naming context held by that server.	100
A RO LDAP server shall not reject search requests whose scope is <i>baseObject</i> when the search filter is a presence match on the objectClass attribute.	101
1.11 Compare Request Processing Requirements	102
Comparison of the assertion value shall be done using the equalityMatch matching rule of the attribute type, if defined.	103
If a request contains a DN with attribute types that the server does not recognize:	104
<ul style="list-style-type: none"> • if the request holds a superior reference then a RO LDAP server shall return a superior reference 	105
<ul style="list-style-type: none"> • otherwise, a RO LDAP server shall return resultCode 32, noSuchObject. 	106

1.12 Requirements for Processing DIT Modification Requests

107

A RO LDAP server shall return the **resultCode** 50 in response to a **ModifyRequest**, **AddRequest**, **DelRequest** or **ModifyDNRequest**, if the client has not previously bound, or bound with the simple authentication choice and a zero length password.

108

Read-Write LDAP Server Profile

109

2.1 Introduction 110

This chapter defines a functional subset of the LDAP protocol definitions to be implemented by LDAP server products. This subset is designed for use by applications that require read and write access to information held in the directory. | 111

Note: Some of the base documents on which this profile is based are currently at Internet Draft status. The reader is warned that the material in these drafts is subject to change. This profile will be updated to reference the RFCs that result from these drafts once they are approved by the IETF. | 112

2.2 References 113

This functional subset of LDAP is defined by the following specifications: | 114

the Read-Only LDAP Server Profile defined in Chapter 1 on page 1 | 115

RFC 1777 116

RFC 2251 117

RFC 2252 118

RFC 2253 119

RFC 2254 120

RFC 2255 121

RFC 2256 122

the **Referrals** Internet Draft 123

the **LDAP over TLS** Internet Draft | 124

the **LDAP Authentication** Internet Draft 125

All statements in these documents listed as “MUST” requirements for a server, with the exception of statements related exclusively to the Modify DN operation, shall be implemented. 126

The following documents are also referenced by this profile: 127

RFC 2222 128

RFC 2195 129

the **UNICODE** Standard 130

ISO 10646 131

RFC 793	132
RFC 791	133
the TLS Internet Draft	134
The ogSupportedProfile attribute referred to in this profile is defined in Chapter 5 on page 23.	135
2.3 General Requirements	136
The phrase <i>RW LDAP server</i> used in this document refers to a product that conforms to this <i>read-write</i> functional subset.	137
A RW LDAP server is defined as a network entity that accepts connections and responds to requests formatted according to the Lightweight Directory Access Protocol made on those connections. The RW LDAP server processes the requests in accordance with the semantics associated with the LDAP operations.	138
If the entity responding to LDAP requests translates these requests into another protocol (such as X.500 DAP) for processing by another network entity, then the RW LDAP server is defined to be the combination of the LDAP translator and all other network-accessible entities that are involved in processing requests.	139
A RW LDAP server shall support the functional subset defined by the <i>Read-Only LDAP Server Profile</i> definition (see Chapter 1 on page 1).	* 140
A RW LDAP server shall support at a minimum the following levels of client authorization:	141
<i>unauthenticated</i> : a client that has not successfully completed a bind operation, or has bound with the simple choice and no password, has this authorization level.	142
<i>administrator</i> : the client is authorized to view all attributes of all entries, and to add, modify and delete entries in a naming context.	143
The requirements in this chapter may be refined and extended by other profiles based on this chapter.	* 144
2.4 Directory Information Tree Requirements	145
A RW LDAP server shall support the return of referrals for superior references, the return of referrals for subordinate references, and the return of search continuation references.	* 146
A RW LDAP server is not required to implement aliases.	* 147
A RW LDAP server shall be capable of having naming contexts, other than a naming context containing a change log, be designated as replicas by the administrator.	148

2.5 Directory Attribute Model Requirements

149

A RW LDAP server that supports one or more of the attribute syntaxes listed in Table 2-1 shall support the use of the attribute option `binary` to define attribute types using these syntaxes.

Syntax	OID
Binary	1.3.6.1.4.1.1466.115.121.1.5
Certificate	1.3.6.1.4.1.1466.115.121.1.8
Certificate List	1.3.6.1.4.1.1466.115.121.1.9
Certificate Pair	1.3.6.1.4.1.1466.115.121.1.10
Supported Algorithms	1.3.6.1.4.1.1466.115.121.1.49

150

Table 2-1 Selected Syntaxes with which the Binary Option can be Used

151
152

2.5.1 Root DSE Requirements

153

In addition to the attributes required by the RO Profile (see Section 1.6.1 on page 3) a RW LDAP server shall provide the following attributes in the root DSE: **supportedControl**, and **supportedExtension**.

154

A RW LDAP server shall provide this value in the **supportedControl** attribute: `2.16.840.1.113730.3.4.2`, for the Manage DSAIT control.

*

155

A RW LDAP server shall provide this value in the **supportedExtension** attribute: `1.3.6.1.4.1.1466.20037`, for the Start TLS extended operation.

156

A RW LDAP server shall provide the values `1.2.826.0.1050.11.1.1` and `1.2.826.0.1050.11.2.1` in the **ogSupportedProfile** attribute.

*

157

2.5.2 Entry Requirements

158

When an entry has been added or modified via LDAP, the server shall provide access to the values of the following attributes as appropriate: **createTimestamp**, **creatorsName**, **modifyTimestamp**, **modifiersName**. Return of values may be subject to access control restrictions.

159

Unless indicated otherwise by the matching rule definition, RW LDAP servers shall accept in values of attributes whose syntax is listed in Table 1-1 on page 6 the UTF-8 encoding of any character from the **UNICODE** Standard.

*

*

160

A RW LDAP server need not support the T.61 character set. The server may reject Add and Modify operations by clients that have bound indicating protocol version 2 which would introduce values of attributes whose syntaxes are listed in Table 1-1 on page 6, when the values contain non-ASCII characters (that is, characters other than those with single-byte UTF-8 encodings in the range 00-7F hex), by returning **resultCode** 21. A RW LDAP server which does support the T.61 character set shall transliterate attribute values in the above syntaxes containing T.61 characters added by LDAP v2 clients to UTF-8 when these values are accessed by LDAP v3 clients.

161

2.5.3	Subschema Entry Requirements	162
	The server shall maintain the modification timestamp in each subschema entry.	163
	The objectClasses attribute shall contain values for the object classes top , subschema and referral . The SUP , MUST and MAY fields in these ObjectClassDescription values shall match the definitions in RFC 2252 and the Referrals Internet Draft, with the exception that the occurrence in the latter document of the attribute name <i>referral</i> is replaced by <i>ref</i> . Additional values of the objectClasses attribute can be present.	164
	The attributeTypes attribute shall contain values for the attribute types objectClass and subschemaSubentry and all attribute types that are present in the root DSE, referral DSEs and the subschema entries. The SUP and SYNTAX fields in these AttributeTypeDescription values shall match the definitions in RFC 2252 and the Referrals Internet Draft. Additional values of the attributeTypes attribute may be present.	165
	A RW LDAP server shall allow additional values of objectClasses and attributeTypes to be added to a subschema entry by a user authorized at the administrator level.	166
2.5.4	Referral DSE Requirements	167
	A RW LDAP server shall support the creation, modification and deletion of DSEs that have the referral object class. Support may be via LDAP modify operations or local means. The server may prevent additions that would cause these DSEs to be non-leaf objects.	* 168
2.6	General Request Processing Requirements	169
	A RW LDAP server shall permit search, compare, abandon, unbind and extended operations to be performed without requiring them to be preceded by a bind operation.	* * 170
2.7	Bind Request Processing Requirements	171
	A RW LDAP server shall support the Simple Authentication and Security Layer (SASL) mechanism <i>CRAM-MD5</i> as described in RFC 2195 . If the bind version is 3, the mechanism name is <i>CRAM-MD5</i> and the credentials field absent, the server shall respond with the resultCode 14 and the serverSaslCreds containing a challenge string. If the bind version is 3, the name field is the name of the entry, the mechanism name is <i>CRAM-MD5</i> , and the credentials field contains the correct hexadecimal digest value for the Distinguished Name and one of the values of the userPassword attribute in the named entry, the server shall respond with the resultCode 0 and the serverSaslCreds field absent.	172
	A RW LDAP server shall support the SASL mechanism <i>EXTERNAL</i> in a bind request following the successful completion of a Start TLS operation (as described in Section 2.12 on page 14). If the client request version field is 3, the name field is absent or contains the same DN as that of the subject of the client's certificate, the mechanism field contains <i>EXTERNAL</i> , and the credentials field is absent, then the server shall attempt to authenticate the user identified by the subject of the client's certificate.	* 173

2.8 Add Request Processing Requirements 174

A RW LDAP server shall accept in Distinguished Names in Add requests any attribute type that is a mandatory or optional attribute of any object class recognized by the server, with the exception of attributes whose syntax requires transfer in binary form. 175

A RW LDAP server may normalize values of attributes with the string-based syntaxes listed in Table 1-1 on page 6. Permitted normalizations are the removal of leading and trailing white space characters. RW LDAP servers that are capable of matching for equality static precomposed and dynamic composed characters and compatibility and non-compatibility characters may normalize values through the conversion of compatibility characters to non-compatibility characters. 176

A RW LDAP server shall ensure that the attribute value assertions in the final RDN component of the DN are present if requested as attributes when the entry is later returned in a search result. 177

A RW LDAP server may change the Distinguished Name of an entry created by a user by reordering the attribute value assertions in multi-valued RDNs. 178

A RW LDAP server shall permit the addition of any entry if the client has authorization at the administrator level, when the parent of the target entry exists, and the proposed entry does not have any schema inconsistencies. 179

A RW LDAP server shall return the **resultCode** 50 in response to a **AddRequest**, if the client is unauthorized. 180

2.9 Modify Request Processing Requirements 181

A RW LDAP server may normalize values of attributes with the string-based syntaxes listed in Table 1-1 on page 6 when added to an entry. Permitted normalizations are the removal of leading and trailing white space characters. RW LDAP servers that are capable of matching for equality static precomposed and dynamic composed characters and compatibility and non-compatibility characters may normalize values through the conversion of compatibility characters to non-compatibility characters. 182

A RW LDAP server shall permit the modification of any user entry in a naming context if the client is authorized at the administrator level and the modification does not introduce any new schema inconsistencies. 183

A RW LDAP server shall return the **resultCode** 50 in response to a **ModifyRequest**, if the client is unauthorized. 184

2.10 Delete Request Processing Requirements 185

A RW LDAP server shall permit the deletion of any leaf entry in a naming context, with the exception of the entry at the base of the naming context, if the client is authorized at the administrator level. 186

A RW LDAP server shall return the **resultCode** 50 in response to a **DelRequest**, if the client is unauthorized. 187

2.11 Modify DN Request Processing Requirements 188

A RW LDAP server shall return the **resultCode** 53 if it does not implement the Modify DN operation. 189

A RW LDAP server shall return **resultCode** 50 in response to a **modDNRequest** if the client is unauthorized. 190

2.12 Protocol Security Requirements 191

A RW LDAP server shall support the Transport Layer Security protocol (TLS, see the **TLS** Internet Draft) and the Start TLS extension. 192

A RW LDAP server shall respond to a TLS client hello in the Secure Sockets Layer (SSL) 3.0 format with a SSL 3.0 server hello. A RW LDAP server shall respond to a TLS version 3.1 client hello with either a TLS 3.1 server hello if it supports TLS, or a SSL 3.0 server hello otherwise. A RW LDAP server need not support SSL version 2.0. 193

A RW LDAP server that responds to a TLS 3.1 client hello with a TLS 3.1 server hello shall implement the cipher suite 194

TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA or 195

TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA.

A RW LDAP server which responds to a TLS 3.1 client hello with a SSL 3.0 server hello shall implement the cipher suite 196

SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA or 197

SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA.

Other cipher suites may also be supported. 198

A RW LDAP server may return a notice of disconnection and close the underlying TCP connection following the receipt of a TLS close notification from the client. 199

White Pages Application LDAP Server Profile

200

3.1 Introduction

201

This chapter defines a functional subset of the LDAP protocol definitions to be implemented by LDAP server products. This subset is designed for use in the white pages application. The white pages schema is derived from the Lightweight Internet Person Schema (LIPS) defined by the Network Applications Consortium (NAC), a version of which is contained in Appendix B on page 27.

202

Note: Some of the base documents on which this profile is based are currently at Internet Draft status. The reader is warned that the material in these drafts is subject to change. This profile will be updated to reference the RFCs that result from these drafts once they are approved by the IETF.

203

3.2 References

204

The following documents are referenced by this profile:

205

the Read-Write LDAP Server Profile defined in Chapter 2 on page 9

206

the Certificate Application LDAP Server Profile defined in Chapter 4 on page 19

207

RFC 1274

208

RFC 2079

209

RFC 2252

210

RFC 2256

211

The **ogSupportedProfile** attribute referred to in this profile is defined in Chapter 5 on page 23.

212

3.3 General Requirements 213

This functional subset of LDAP is to be used in combination with the Read-Write LDAP Server Profile Definition and the Certificate Application LDAP Server Profile Definition. All requirements from these profile definitions are incorporated by reference. 214

The server shall provide the value 1.2.826.0.1050.11.3.1 in the **ogSupportedProfile** attribute of the root DSE. 215

3.4 Schema Requirements 216

An LDAP server implementing this profile shall support the schema elements described in this section. For each attribute listed, the server shall also implement the syntax and matching rule definitions associated with the attribute. 217

The following object classes defined in **RFC 2256** shall be supported: 218

- certificationAuthority**
- certificationAuthority-V2**
- cRLDistributionPoint**
- country**
- locality**
- organization**
- organizationalUnit**
- organizationalPerson**
- person**
- residentialPerson**
- top**

The following object classes shall be supported by the server. 219 | 220

Note: They are derived from the NAC LIPS. 221 | 221

```
(1.3.6.1.4.1.1466.154.151.160.1
  NAME 'liPerson'
  SUP person
  MAY (rfc822Mailbox $ userCertificate $ labeledURI $
    givenName $ generationQualifier $ o $ l $ c $
    personalTitle $ initials $ middleName $
    uniqueIdentifier $ homeTelephoneNumber $ homeFax $
    homePostalAddress $ thumbnailPhoto $ title $
    facsimileTelephoneNumber $ mobileTelephoneNumber $
    pagerTelephoneNumber $
    postalAddress $ ou $ roomNumber $ otherMailbox $
    telexNumber $ thumbnailLogo $ secretary $ manager $
    description $ telephoneNumber $ userPassword) 222
```

```
(1.3.6.1.4.1.1466.154.151.160.2
  NAME 'liOrganization'
  SUP organization
  MAY (rfc822Mailbox $ labeledURI $ c $ uniqueIdentifier $
    otherMailbox $ thumbnailLogo $ manager) 223
```

The following attributes defined in **RFC 2252** shall be maintained by the server: 224

createTimestamp
creatorsName
modifiersName
modifyTimestamp

The following attributes defined in **RFC 1274** shall be supported: 225

homeTelephoneNumber
homePostalAddress
rfc822Mailbox
manager
otherMailbox
mobileTelephoneNumber
pagerTelephoneNumber
personalTitle
roomNumber
secretary
uniqueIdentifier

226

The following attribute defined in **RFC 2079** shall be supported: 227

labeledURI

228

The following attributes defined in **RFC 2256** shall be supported: 229

authorityRevocationList	ou
businessCategory	physicalDeliveryOfficeName
c	postalAddress
caCertificate	postalCode
certificateRevocationList	postOfficeBox
cn	preferredDeliveryMethod
crossCertificatePair	registeredAddress
deltaRevocationList	searchGuide
description	seeAlso
destinationIndicator	sn
facsimileTelephoneNumber	st
generationQualifier	street
givenName	telephoneNumber
initials	teletexTerminalIdentifier
InternationaliSDNNumber	telexNumber
l	title
o	userCertificate
objectClass	userPassword
	x121Address

230

The following attributes defined in **RFC 2256** shall be supported in search and compare operations (servers need not permit them to be added to entries): 231

distinguishedName
name

232

The following attributes shall be supported by the server. 233

234

(1.3.6.1.4.1.1466.101.120.31 NAME 'homeFax' EQUALITY telephoneNumberMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.22)	235
(2.16.128.113533.1.1400.1 NAME 'thumbnailPhoto' SYNTAX 1.3.6.1.4.1.1466.115.121.1.28)	* 236
(2.16.128.113533.1.1400.2 NAME 'thumbnailLogo' SYNTAX 1.3.6.1.4.1.1466.115.121.1.28)	237
(1.3.6.1.4.1.1466.101.120.34 NAME 'middleName' SUP name)	238

Certificate Application LDAP Server Profile

239

4.1 Introduction 240

This chapter defines a functional subset of the LDAP protocol definitions to be implemented by LDAP server products. This subset is designed for use in the certificate storage and retrieval application, and is based on the **PKIX LDAPv2** Internet Draft, which profiles use of the protocol LDAP v2.

241

Note: Some of the base documents on which this profile is based are currently at Internet Draft status. The reader is warned that the material in these drafts is subject to change. This profile will be updated to reference the RFCs that result from these drafts once they are approved by the IETF.

242

4.2 References 243

The following documents are referenced by this profile:

244

the Read-Write LDAP Server Profile defined in Chapter 2 on page 9

245

the **PKIX LDAPv2** Internet Draft

246

RFC 2252

247

RFC 2256

248

The **ogSupportedProfile** attribute referred to in this profile is defined in Chapter 5 on page 23.

249

4.3 General Requirements 250

This functional subset of LDAP is to be used in combination with the Read-Write LDAP Server Profile Definition.

* 251

All requirements from the LDAP Repository Read, LDAP Repository Search and LDAP Repository Modify sections of the **PKIX LDAPv2** Internet Draft shall be supported by an LDAP server following this profile. This implies that an LDAP server conforming to this profile shall support LDAP v2.

252

The server shall provide the value 1.2.826.0.1050.11.4.1 in the **ogSupportedProfile** attribute of the root DSE.

253

4.4 Schema Requirements

254

An LDAP server implementing this profile shall support the schema elements described in this section. For each attribute listed, the server shall implement the underlying syntax definition, and the equality matching rule, if such rule is contained in the attribute definition.

255

The following object classes defined in **RFC 2256** shall be supported:

256

certificationAuthority
certificationAuthority-V2
cRLDistributionPoint
country
locality
organization
organizationalUnit
organizationalPerson
person
residentialPerson
top

The following attributes defined in **RFC 2252** shall be maintained by the server:

257

258

createTimestamp
creatorsName
modifiersName
modifyTimestamp

The following attributes defined in **RFC 2256** shall be supported:

259

260

authorityRevocationList	ou
businessCategory	physicalDeliveryOfficeName
c	postalAddress
caCertificate	postalCode
certificateRevocationList	postOfficeBox
cn	preferredDeliveryMethod
crossCertificatePair	registeredAddress
deltaRevocationList	searchGuide
description	seeAlso
destinationIndicator	sn
facsimileTelephoneNumber	st
generationQualifier	street
givenName	telephoneNumber
initials	teletexTerminalIdentifier
InternationaliSDNNumber	telexNumber
l	title
o	userCertificate
objectClass	userPassword
	x121Address

261

4.5 Attributes Requiring Special Handling 262

The following attributes require special handling in Search, Add and Modify operations. 263

authorityRevocationList
caCertificate
certificateRevocationList
crossCertificatePair
deltaRevocationList
userCertificate

An LDAP server shall always return values of these attributes in binary form, never as a string encoding. When a client has bound using protocol version 2, the server shall return the attributes with all description options removed. When the client has bound using protocol version 3 or has not bound, the server shall return the attributes with the *binary* description option present on attributes of these types in the search result entries. 264
265

An LDAP server shall treat the attribute types and their subtype with the *binary* description option as equivalent when evaluating search filters and performing Add and Modify operations. 266

4.6 Bind Operation Requirements 267

An LDAP server shall support the simple authentication choice with LDAP versions 2 and 3. The server will check the client's presented distinguished name and password, and ensure that the password is present as a value of the **userPassword** attribute in that entry. The equality matching rule of the **userPassword** attribute is used to evaluate the comparison between a presented and stored value. 268

The *ogSupportedProfile* Attribute

269

The **ogSupportedProfile** attribute is defined as follows.

270

```
(1.2.826.0.1050.11.0  
  NAME 'ogSupportedProfile'  
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.38)
```

271

The values of the **ogSupportedProfile** attribute are OIDs identifying the LDAP profiles that the server supports.

272

Object Identifier Assignment

The object identifiers for the **ogSupportedProfile** attribute and its values stem from the root: iso(1) national-member-body(2) uk (826) national(0) xopen(1050) ldap-profiles(11). All extensions of this OID are reserved for use in connection with LDAP profiles.

274

OID 1.2.826.0.1050.11.0 is assigned to identify the **ogSupportedProfile attribute**.

275

OIDs extending 1.2.826.0.1050.11.1 are reserved to identify versions of the Read-Only LDAP Server Profile.

276

OIDs extending 1.2.826.0.1050.11.2 are reserved to identify versions of the Read-Write LDAP Server Profile.

277

OIDs extending 1.2.826.0.1050.11.3 are reserved to identify versions of the White Pages Application LDAP Server Profile.

278

OIDs extending 1.2.826.0.1050.11.4 are reserved to identify versions of the Certificate Application LDAP Server Profile.

279

OIDs extending 1.2.826.0.1050.11.5 are reserved to identify versions of the Single Sign On Application LDAP Server Profile.

280

Object Identifiers are assigned to the profiles defined in this document as follows.

281

Profile	OID
Read-Only LDAP Server	1.2.826.0.1050.11.1.1
Read-Write LDAP Server	1.2.826.0.1050.11.2.1
White Pages Application LDAP Server	1.2.826.0.1050.11.3.1
Certificate Application LDAP Server	1.2.826.0.1050.11.4.1

282

The Lightweight Internet Person Schema (LIPS)

283

The Lightweight Internet Person Schema (LIPS) was defined by the Network Applications Consortium (NAC).² This Appendix contains the version of 20 February 1997.

284

General Attributes

285

Generic Name		NAC LIP Schema	
1	Electronic Mail	1	mail
2	Certificate	2	userCertificate
3	Uniform Resource Locator	3	labeledURI
4	Full Name	4	cn
5	Given Name	5	givenName
6	Last Name	6	sn
7	Generation Qualifier	7	generationQualifier
8	Organization	8	o
9	City	9	l
10	Country	10	c
11	Personal Title	11	personalTitle
12	Initials	12	initials
13	Middle Name	13	middleName
14	Unique Identifier	14	uniqueIdentifier

286

Personal Attributes

287

Generic Name		NAC LIP Schema	
15	Home Telephone Number	15	homePhone
16	Home Fax	16	homeFax
17	Home Postal Address	17	homePostalAddress
18	Description	18	description
19	Personal Photograph	19	thumbnailPhoto

288

2. Information about the NAC is available from the NAC Web Site at <http://www.netapps.org>.

Organizational Attributes

289 |

Generic Name		NAC LIP Schema	
20	Title	20	title
21	Office Telephone Number	21	telephoneNumber
22	Office Fax Number	22	facsimileTelephoneNumber
23	Office Mobile Telephone Number	23	mobileTelephoneNumber
24	Office Pager Number	24	pager
25	Postal Address	25	postalAddress
26	Organizational Department	26	ou
27	Room Number	27	physicalDeliveryOfficeName
28	E-mail Address	28	textEncodedORaddress
29	Telex Telephone Number	29	telexNumber
30	Company Logo	30	thumbnailLogo
31	Secretary	31	secretary
32	Manager	32	manager

290 |

Security

291 |

Generic Name		NAC LIP Schema	
33	User Password	33	userPassword

292 |

Ancillary

293 |

Generic Name		NAC LIP Schema	
34	Creation Time	34	createTimestamp
35	Last Modified	35	modifyTimestamp
36	Creators Name	36	creatorsName
37	Modifiers Name	37	modifiersName

294 |

Glossary

ASCII

American Standard Code for Information Interchange. A 7-bit encoding of the English alphabet (upper and lower case letters), plus numerals, plus punctuation characters, plus a few special characters (such as '\$' and '#'), plus characters that affect operation of a printing device or communications channel (control characters). The **Unicode** encodings of the characters that have ASCII encodings, considered as integers in range 0-127, are the same as the ASCII encodings.

295

Attribute

An attribute is a type with one or more associated values. The attribute type is identified by a short descriptive name and an **OID**. It governs whether there can be more than one value of an attribute of that type in an entry, the syntax to which the values must conform, the kinds of matching that can be performed on values of that attribute, and other functions.

296

Attribute Type

The type of an **Attribute**.

297

Attribute Value Assertion (AVA)

A proposition, which may be true, false or undefined, concerning the values of an **Entry**.

298

AVA

Abbreviation for **Attribute Value Assertion**.

299

Certificate Profile

The Application LDAP Server Profile defined in Chapter 4 on page 19.

300

DAP

Abbreviation for "Directory Access Protocol". **LDAP** and the **X.500 DAP** are examples of DAPs.

301

Directory Information Base (DIB)

The complete set of information to which the directory provides access and which includes all the pieces of information that can be read or manipulated using the operations of the directory. It is made up of **Entries**.

302

Directory Information Tree

The **Directory Information Base** considered as a tree, whose vertices (other than the root) are the directory **Entries**.

303

Directory Server

A network entity that accepts connections and responds to requests formatted according to **LDAP** made on those connections.

304

Distinguished Name (DN)

The concatenation of the **RDNs** of the sequence of **Entries** from a particular entry to an immediate subordinate of the root of the **DIT** forms that entry's Distinguished Name, which is unique in the **DIT**.

305

DN

Abbreviation for **Distinguished Name**.

306

DIT

Abbreviation for **Directory Information Tree**.

307

DSA-Specific Entry (DSE)	
An entry specific to a Directory Server (“DSA” is an X.500 term for a directory server.)	308
DSE	
Abbreviation for DSA-Specific Entry	309
Entry	
The part of the Directory Information Base containing information relating to a single Object . Each entry is made up of <i>Attributes</i> .	310
IANA	
The Internet Assigned Numbers Authority. See http://www.iana.org .	311
IETF	
The Internet Engineering Task Force. See http://www.ietf.org .	312
IP version 4	
Version 4 of the Internet Protocol, defined in RFC 791 .	313
IP version 6	
The New Generation Internet Protocol that is (in 1998) in course of definition by the IETF .	314
ISO/IEC	
The International Organization for Standardization (ISO, see http://www.iso.ch) and the International Electrotechnical Commission (IEC, see http://www.iec.ch). These two bodies formed a Joint Technical Committee (JTC1) that has been responsible for the production of a number of International Standards for information processing.	315
ITU-T	
The Telecommunication Standardization Sector of the International Telecommunications Union, see http://www.itu.ch .	316
IWP	
Abbreviation for Internet White Pages .	317
IWP Profile	
White Pages Profile .	318
LDAP	
Lightweight Directory Access Protocol, as defined in RFC 1777 (LDAP Version 2) or RFC 2251 (LDAP Version 3).	319
LIPS	
Lightweight Internet Person Schema, see Appendix B on page 27.	320
NAC	
The Network Applications Consortium, see http://www.netapps.org .	321
Naming Context	
The largest collection of Entries , starting at an entry that is mastered by a particular server, and including all its Subordinates and their subordinates, down to the entries that are mastered by different servers, is termed a naming context.	322
Object	
Anything that is identifiable (can be named), and that it is of interest to hold information on in the Directory Information Base .	323
Object Class	
An identified family of Objects that share certain characteristics.	324

Object Identifier (OID)	
A value (distinguishable from all other such values) that is associated with an information object. OIDs are sequences of numbers that are uniquely assigned to objects in a manner prescribed by International Standards (see ISO 8824).	325
OID	
Abbreviation for Object Identifier	326
Operational Attribute	
Operational attributes are Attributes used by servers for administering the directory system itself. They are not returned in search results unless explicitly requested by name.	327
Relative Distinguished Name (RDN)	
One or more attribute values from an Entry form its Relative Distinguished Name (RDN), which must be unique among all its siblings in the DIT .	328
RDN	
Abbreviation for Relative Distinguished Name .	329
RO	
Abbreviation for “Read-Only”.	330
RO LDAP Server	
A server that conforms to the Read-Only LDAP Server Profile defined in Chapter 1 on page 1.	331
Root DSE	
The root of the DIT is a DSA-specific Entry and not part of any naming context : each server has different attribute values in the root DSE.	332
RW	
Abbreviation for “Read-Write”.	333
RW LDAP server	
A server that conforms to the Read-Write LDAP Server Profile defined in Chapter 2 on page 9.	334
SASL	
Simple Authentication and Security Layer, see RFC 2222 .	335
Schema	
A Schema is the collection of attribute type definitions, object class definitions and other information that a server uses to determine how to match a filter or Attribute Value Assertion (in a compare operation) against the Attributes of an Entry , and whether to permit add and modify operations.	336
SSL	
The Secure Sockets Layer transport security protocol, see the SSL specification. TLS is based on SSL.	337
Subordinate	
In the DIT , an Entry is subordinate to another if the other entry is Superior to it.	338
Subschema Entry	
Subschema entries are Entries used for administering information about the directory Schema , in particular the Object Classes and Attribute Types supported by directory servers. A single subschema entry contains all schema definitions used by entries in a particular part of the DIT .	339
Superior	
In the DIT , an Entry is superior to another if it is on the path between the other entry and the root. Each entry has exactly one immediate superior, whose distinguished name followed by the RDN of the entry forms the distinguished name of the entry.	340

T.61	The character encoding scheme defined in ITU-T Recommendation T.61 . This is an extension of ASCII that caters for national characters from a restricted number of languages in addition to English.	341
TCP	The Transmission Control Protocol of the Internet, defined in RFC 793 .	342
TLS	The Transport Layer Security protocol of the IETF , see the TLS Internet Draft.	343
Unicode	The character encoding scheme defined in the UNICODE Standard. This is an encoding scheme that caters for national characters from most languages in addition to English. It encodes each character in 16 bits. ISO 10646 defines an extension of Unicode that encodes each character in 16 bits or 32 bits and is intended to cater for all characters that may be used anywhere in the world.	344
US-ASCII	The ASCII character encoding. The term <i>US-ASCII</i> emphasizes that national variations (such as the substitution of the UK pound sign for the '#' character, as in "UK-ASCII") are not used.	345
UTF-8	A Universal Character Set (UCS) Transformation Format in which each 16-bit or 32-bit character encoding of ISO 10646 is transformed into a 1, 2, 3, 4 or 5-byte encoding. UTF-8 has the property that the UTF-8 encodings of the first 128 characters are the same as their ASCII encodings and that, except for the null character itself (which has encoding 0), no character encoding contains a null byte.	346
White Pages Profile	The Application LDAP Server Profile defined in Chapter 3 on page 15.	347
Whitespace Character	A character whose representation leaves no mark on the printed page. For the purposes of this document, the whitespace characters are listed in Table 1-2 on page 6.	348
X.500	The X.500 series of ITU-T recommendations and International Standards, and the directory model, services and protocols that they define.	349
X.500 DAP	The Directory Access Protocol (DAP) in X.500 .	350

Index

Add operation	1	close connection.....	4, 14
Add Request Processing Requirements		cn attribute.....	17, 20
RW Profile	13	cn LIPS attribute	27
AddRequest	13	Company Logo general attribute	28
administrator	3, 5, 12-14	Compare Request Processing Requirements	
authorization level	10	RO Profile	7
aliases	2, 10	compatibility characters.....	7, 13
ASCII.....	29	connection close.....	4, 14
Attribute	29	context prefix.....	7
Attribute Type	29	controlType field.....	4
Attribute Value Assertion (AVA).....	29	Country general attribute	27
AttributeTypeDescription.....	3	country object class.....	16, 20
attributeTypes attribute.....	3, 12	Country String syntax.....	6
authentication.....	21	CRAM-MD5 SASL mechanism	12
authMethodNotSupported.....	5	createTimestamp attribute	11, 17, 20
authorityRevocationList attribute.....	17, 20-21	createTimestamp attribute type	5
authorization	10	createTimestamp LIPS attribute.....	28
AVA.....	29	Creation Time general attribute	28
baseObject field.....	7	Creators Name general attribute.....	28
binary attribute option	11	creatorsName attribute	11, 17, 20
binary form	13, 21	creatorsName LIPS attribute.....	28
Binary syntax.....	11	critical controls.....	4
bind operation.....	4, 12	cRLDistributionPoint object class.....	16, 20
Bind Operation Requirements		crossCertificatePair attribute.....	17, 20-21
Certificates Profile	21	DAP	29
Bind Request Processing Requirements		Delete operation.....	1
RO Profile	5	Delete Request Processing Requirements	
RW Profile	12	RW Profile.....	14
businessCategory attribute	17, 20	DelRequest	14
c attribute	17, 20	deltaRevocationList attribute.....	17, 20-21
c LIPS attribute.....	27	description attribute	17, 20
caCertificate attribute	17, 20-21	Description general attribute	27
Certificate Application LDAP Server Profile		description LIPS attribute	27
OID assignment	25	destinationIndicator attribute.....	17, 20
Certificate general attribute.....	27	Directory Attribute Model Requirements	
Certificate List syntax.....	11	RO Profile	3
Certificate Pair syntax.....	11	RW Profile.....	11
Certificate Profile.....	19, 29	Directory Information Base (DIB)	29
Certificate syntax.....	11	Directory Information Tree.....	29
certificateRevocationList attribute.....	17, 20-21	Directory Information Tree Requirements	
certificationAuthority-V2 object class.....	20	RO Profile	2
certificationAuthority object class	16, 20	RW Profile.....	10
certificationAuthority-V2 object class.....	16	Directory Server.....	29
cipher suites.....	14	Directory String syntax.....	6
City general attribute.....	27	Distinguished Name	13
client authorization	10	Distinguished Name (DN).....	29

Distinguished Name Requirements	
RO Profile	4
distinguished names	
comparison	4
distinguishedName attribute	17
DIT	29
DIT Modification Request Processing Requirements	
RO Profile	8
DN	29
dnAttributes field	7
DSA-Specific Entry (DSE)	30
DSE	30
root	11
dynamically composed characters	7, 13
E-mail Address general attribute	28
Electronic Mail general attribute	27
Entry	30
Entry Requirements	
RO Profile	3
RW Profile	11
equalityMatch	7
ExtendedRequest	4
extensibleMatch	7
EXTERNAL SASL mechanism	12
Facsimile Telephone Number syntax	6
facsimileTelephoneNumber attribute	17, 20
facsimileTelephoneNumber LIPS attribute	28
Full Name general attribute	27
General Request Processing Requirements	
RO Profile	4
RW Profile	12
General Requirements	
Certificates Profile	19
IWP Profile	16
RO Profile	2
RW Profile	10
Generation Qualifier general attribute	27
generationQualifier attribute	17, 20
generationQualifier LIPS attribute	27
Given Name general attribute	27
givenName attribute	17, 20
givenName LIPS attribute	27
greaterOrEqual filter	5
Home Fax general attribute	27
Home Postal Address general attribute	27
Home Telephone Number general attribute	27
homeFax attribute	18
homeFax LIPS attribute	27
homePhone LIPS attribute	27
homePostalAddress attribute	17
homePostalAddress LIPS attribute	27
homeTelephoneNumber attribute	17
IANA	30
IETF	30
initials attribute	17, 20
Initials general attribute	27
initials LIPS attribute	27
InternationaliSDNNumber attribute	17, 20
IP version 4	2, 30
IP version 6	2, 30
ISO/IEC	30
ITU-T	30
IWP	30
IWP Profile	30
l attribute	17, 20
l LIPS attribute	27
labeledURI attribute	17
labeledURI LIPS attribute	27
Last Modified general attribute	28
Last Name general attribute	27
LDAP	30
lessOrEqual filter	5
liOrganization object class	16
liPerson object class	16
LIPS	30
locality object class	16, 20
mail LIPS attribute	27
Manage DSAIT control	11
manager attribute	17
Manager general attribute	28
manager LIPS attribute	28
matching	5-7
matchingRule field	7
Middle Name general attribute	27
middleName attribute	18
middleName LIPS attribute	27
mobileTelephoneNumber attribute	17
mobileTelephoneNumber LIPS attribute	28
modDNRequest	14
modification timestamp	12
Modifiers Name general attribute	28
modifiersName attribute	11, 17, 20
modifiersName LIPS attribute	28
Modify DN operation	1, 9
Modify DN Request Processing Requirements	
RW Profile	14
Modify operation	1
Modify Request Processing Requirements	
RW Profile	13
ModifyRequest	13
modifyTimestamp attribute	11, 17, 20

Index

modifyTimestamp attribute type	5
modifyTimestamp LIPS attribute.....	28
multi-valued RDNs.....	4
NAC.....	30
name attribute	17
naming context.....	2
Naming Context	30
namingContexts attribute.....	3
Network Requirements	
RO Profile.....	2
non-compatibility characters	7, 13
normalization	13
noSuchObject result code	5, 7
Numeric String syntax.....	6
o attribute.....	17, 20
o LIPS attribute	27
Object	30
Object Class	30
Object Identifier (OID).....	31
Object Identifier Assignment	25
objectClass attribute	3, 7, 17, 20
objectClassDescription	3, 12
objectClasses attribute.....	3, 12
objectClass attribute type	12
Office Fax Number general attribute.....	28
Office Mobile Telephone Number general attribute.....	28
Office Pager Number general attribute.....	28
Office Telephone Number general attribute	28
ogSupportedProfile attribute.....	3, 16, 19, 23, 25
ogSupportedProfile attribute	11
OID	31
OID Assignment	25
Operational Attribute	31
Organization general attribute	27
organization object class	16, 20
Organizational Department general attribute.....	28
organizationalPerson object class	16, 20
organizationalUnit object class	16, 20
otherMailbox attribute	17
ou attribute	17, 20
ou LIPS attribute	28
pager LIPS attribute	28
pagerTelephoneNumber attribute	17
person object class.....	16, 20
Personal Photograph general attribute	27
Personal Title general attribute.....	27
personalTitle attribute	17
personalTitle LIPS attribute	27
physicalDeliveryOfficeName attribute	17, 20
physicalDeliveryOfficeName LIPS attribute	28
Postal Address general attribute	28
Postal Address syntax.....	6
postalAddress attribute	17, 20
postalAddress LIPS attribute	28
postalCode attribute	17, 20
postOfficeBox attribute	17, 20
precomposed characters	7, 13
preferredDeliveryMethod attribute.....	17, 20
Printable String syntax	6
Protocol Security Requirements	
RW Profile	14
protocolError	4
quoting.....	4
RDN.....	31
Read-Only LDAP Server Profile	10
OID assignment	25
Read-Only Profile	1
read-write functional subset	10
Read-Write LDAP Server Profile	
OID assignment	25
Read-Write Profile	9
referral.....	2, 4
Referral DSE Requirements	
RW Profile	12
referral object class	12
referrals.....	3, 10
registeredAddress attribute	17, 20
Relative Distinguished Name (RDN).....	31
replicas.....	10
residentialPerson object class	16, 20
rfc822Mailbox attribute	17
RO	31
RO LDAP Server.....	2, 31
Room Number general attribute	28
roomNumber attribute.....	17
root DSE.....	2, 11
Root DSE.....	31
Root DSE Requirements	
RO Profile	3
RW Profile	11
RW	31
RW LDAP server	10, 31
RW Profile	19
SASL.....	31
Schema.....	31
Schema Requirements	
Certificates Profile	20
IWP Profile.....	16
search continuation references.....	2, 4, 10
Search Filter Processing Requirements	
RO Profile	5

search filtering.....	5	thumbnailPhoto attribute	18
Search Request Processing Requirements		thumbnailPhoto LIPS attribute.....	27
RO Profile	5	title attribute	17, 20
searchGuide attribute	17, 20	Title general attribute	28
searchResultEntry.....	4	title LIPS attribute.....	28
secretary attribute.....	17	TLS.....	14, 32
Secretary general attribute.....	28	top object class	12, 16, 20
secretary LIPS attribute	28	type field.....	7
Security Requirements		unauthenticated	
Protocol.....	14	authorization level	10
seeAlso attribute.....	17, 20	Unicode.....	32
serverSaslCreds.....	12	Uniform Resource Locator general attribute	27
Single Sign On Application LDAP Server Profile		Unique Identifier general attribute	27
OID assignment	25	uniqueIdentifier attribute	17
sn attribute	17, 20	uniqueIdentifier LIPS attribute.....	27
sn LIPS attribute.....	27	unparsable requests	4
SSL.....	14, 31	unrecognized attribute types	5
st attribute.....	17, 20	US-ASCII	32
Start TLS extended operation	11	User Password general attribute	28
Start TLS extension.....	14	userCertificate attribute.....	17, 20-21
street attribute	17, 20	userCertificate LIPS attribute.....	27
Subordinate.....	31	userPassword attribute	12, 17, 20-21
subschema entry	2	userPassword LIPS attribute.....	28
Subschema Entry	31	UTF-8.....	32
Subschema Entry Requirements		White Pages Application LDAP Server Profile	
RO Profile	3	OID assignment	25
RW Profile	12	White Pages Profile	15, 32
subschema object class	12	Whitespace Character.....	32
subschemaSubentry	3	X.500	32
subschemaSubentry attribute	3	X.500 DAP	2, 10, 32
subschemaSubentry attribute type	12	x121Address attribute	17, 20
Superior	31		
superior reference.....	5, 7		
Supported Algorithms syntax	11		
supportedControl attribute	11		
supportedExtension attribute	11		
supportedExtension attribute	11		
supportedLDAPVersion attribute	3		
T.61.....	32		
T.61 character set.....	11		
TCP	2, 32		
Telephone Number syntax	6		
telephoneNumber attribute	17, 20		
telephoneNumber LIPS attribute	28		
teletexTerminalIdentifier attribute.....	17, 20		
Telex Telephone Number general attribute	28		
telexNumber attribute.....	17, 20		
telexNumber LIPS attribute	28		
textEncodedORaddress LIPS attribute	28		
thumbnailLogo attribute.....	18		
thumbnailLogo LIPS attribute	28		