

INTERNET-DRAFT

Intended Category:

Standards Track

Updates: [2251](#), [2252](#), [2253](#), [2254](#),
[2255](#), [2256](#), [2829](#), [2830](#)

Jeff Hodges, Oblix Inc.

RL "Bob" Morgan, Univ of Washington

October, 2000

Lightweight Directory Access Protocol (v3):
Technical Specification

<[draft-hodges-ldapbis-ldapv3-ts-00.txt](#)>

Status of this Document

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet- Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

Comments and suggestions on this document are encouraged. Comments on this document should be sent to the LDAPbis BOF discussion list:

ietf-ldapbis@OpenLDAP.org

This document expires in May 2001.

Abstract

This document specifies the set of RFCs comprising LDAPv3, and documents the addressing of the "IESG Note" attached to RFCs 2251 through 2256.

1. Background and Motivation

The specification for the Lightweight Directory Access Protocol version **3** (LDAPv3) nominally comprises eight RFCs which were issued in two distinct subsets at separate times (RFCs 2251 through 2256 first, then RFCs **2829** and **2830** following later).

RFCs 2251 through 2256 are each embellished with an "IESG Note" (Note) warning implementors and deployers of potential interoperability problems due to the lack of a specification of mandatory-to-implement authentication mechanism(s).

The purpose of this document is to remedy both issues by explicitly specifying the set of RFCs comprising LDAPv3 and documenting the fact that the IESG now considers the "IESG Note" as "addressed" given the specification of mandatory-to-implement authentication mechanisms in RFC 2829.

2. Conventions Used in this Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

3. Specification of LDAPv3

The Lightweight Directory Access Protocol version 3 (LDAPv3) is specified by this set of nine RFCs:

- [RFC2251] Lightweight Directory Access Protocol (v3)
[the specification of the LDAP on-the-wire protocol]
- [RFC2252] Lightweight Directory Access Protocol (v3):
Attribute Syntax Definitions
- [RFC2253] Lightweight Directory Access Protocol (v3):
UTF-8 String Representation of Distinguished Names
- [RFC2254] The String Representation of LDAP Search Filters
- [RFC2255] The LDAP URL Format
- [RFC2256] A Summary of the X.500(96) User Schema for use
with LDAPv3
- [RFC2829] Authentication Methods for LDAP

[RFC2830] Lightweight Directory Access Protocol (v3):
Extension for Transport Layer Security

And, this document (RFCxxxx).

The term "LDAPv3" MAY be used to informally refer to the protocol specified by this set of RFCs. The LDAPv3 protocol suite, as defined here, SHOULD be formally referenced by a normative reference to this document.

Other RFCs (and perhaps Internet-Drafts) MAY specify extensions to LDAPv3. Nomenclature denoting such combinations of LDAPv3-plus-extension(s) is not defined by this document, and MAY be defined in some future document(s).

4. Addressing the "IESG Note" on RFCs 2251 through 2256

The IESG approved publishing RFCs 2251 through 2256 with an attendant Note included in each document. The Note begins with..

This document describes a directory access protocol that provides both read and update access. Update access requires secure authentication, but this document does not mandate implementation of any satisfactory authentication mechanisms.

The Note ends with this statement..

Implementors are hereby discouraged from deploying LDAPv3 clients or servers which implement the update functionality, until a Proposed Standard for mandatory authentication in LDAPv3 has been approved and published as an RFC.

[RFC2829] is the "Proposed Standard for mandatory authentication in LDAPv3" called for in the Note. Therefore, the IESG considers the Note on [[RFC2251](#)], [[RFC2252](#)], [[RFC2253](#)], [[RFC2254](#)], [[RFC2255](#)], and [[RFC2256](#)] as being addressed.

5. Security Considerations

This document does not directly discuss security, although the context of the aforementioned "IESG Note" is security related, as is the manner in which the Note is addressed.

Please refer to the referenced documents, especially [[RFC2829](#)], [[RFC2251](#)], and [[RFC2830](#)], for further information concerning LDAPv3 security.

6. Acknowledgements

The authors thank Patrick Falstrom, Leslie Daigle, and Kurt Zeilenga for their contributions to this document.

7. References

- [RFC2119] Scott Bradner. "Key Words for use in RFCs to Indicate Requirement Levels". [RFC 2119](#), March 1997.
- [RFC2251] M. Wahl, S. Kille and T. Howes, "Lightweight Directory Access Protocol (v3)", [RFC 2251](#), December 1997.
- [RFC2252] M. Wahl, A. Coulbeck, T. Howes, and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", [RFC 2252](#), December 1997.
- [RFC2253] S. Kille, M. Wahl, and T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", [RFC 2253](#), December 1997.
- [RFC2254] T. Howes, "The String Representation of LDAP Search Filters", [RFC 2254](#), December 1997.
- [RFC2255] T. Howes, M. Smith, "The LDAP URL Format", [RFC 2255](#), December 1997.
- [RFC2256] M. Wahl, "A Summary of the X.500(96) User Schema for use with LDAPv3", [RFC 2256](#), December 1997.
- [RFC2829] M. Wahl, H. Alvestrand, J. Hodges, R. Morgan. "Authentication Methods for LDAP", [RFC 2829](#), May 2000.
- [RFC2830] J. Hodges, R. Morgan, M. Wahl, "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security", [RFC 2830](#), May 2000.

8. Authors' Addresses

Jeff Hodges
Obliv, Inc.
18922 Forge Drive
Cupertino, CA 95014
USA

Phone: +1-408-861-6656
EMail: JHodges@obliv.com

RL "Bob" Morgan
Computing and Communications
University of Washington
Seattle, WA
USA

Phone: +1-206-221-3307
EMail: rlmorgan@washington.edu

9. Intellectual Property Rights Notices

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

10. Copyright Notice and Disclaimer

Copyright (C) The Internet Society (1998). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This document expires in January 2001.

