Network Working Group
Request for Comments: 4370
Category: Standards Track

R. Weltman
Yahoo!, Inc.

February 2006

# Lightweight Directory Access Protocol (LDAP) Proxied Authorization Control

## Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

## Copyright Notice

Copyright (C) The Internet Society (2006).

## Abstract

This document defines the Lightweight Directory Access Protocol (LDAP) Proxy Authorization Control. The Proxy Authorization Control allows a client to request that an operation be processed under a provided authorization identity instead of under the current authorization identity associated with the connection.

## 1. Introduction

Proxy authorization allows a client to request that an operation be processed under a provided authorization identity instead of under the current authorization identity associated with the connection. This document defines support for proxy authorization using the Control mechanism [RFC2251]. The Lightweight Directory Access Protocol [LDAPV3] supports the use of the Simple Authentication and Security Layer [SASL] for authentication and for supplying an authorization identity distinct from the authentication identity, where the authorization identity applies to the whole LDAP session. The Proxy Authorization Control provides a mechanism for specifying an authorization identity on a per-operation basis, benefiting clients that need to perform operations efficiently on behalf of multiple users.

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" used in this document are to be interpreted as described in [KEYWORDS].

## 2. Publishing Support for the Proxy Authorization Control

Support for the Proxy Authorization Control is indicated by the presence of the Object Identifier (OID) "2.16.840.1.113730.3.4.18" in the supportedControl attribute [RFC2252] of a server's root DSA-specific Entry (DSE).

## 3. Proxy Authorization Control

A single Proxy Authorization Control may be included in any search, compare, modify, add, delete, or modify Distinguished Name (DN) or extended operation request message. The exception is any extension that causes a change in authentication, authorization, or data confidentiality [RFC2829], such as Start TLS [LDAPTLS] as part of the controls field of the LDAPMessage, as defined in [RFC2251].

The controlType of the proxy authorization control is "2.16.840.1.113730.3.4.18".

The criticality MUST be present and MUST be TRUE. This requirement protects clients from submitting a request that is executed with an unintended authorization identity.

Clients MUST include the criticality flag and MUST set it to TRUE. Servers MUST reject any request containing a Proxy Authorization Control without a criticality flag or with the flag set to FALSE with a protocolError error. These requirements protect clients from submitting a request that is executed with an unintended authorization identity.

The controlValue SHALL be present and SHALL either contain an authzId [AUTH] representing the authorization identity for the request or be empty if an anonymous association is to be used.

The mechanism for determining proxy access rights is specific to the server's proxy authorization policy.

If the requested authorization identity is recognized by the server, and the client is authorized to adopt the requested authorization identity, the request will be executed as if submitted by the proxy authorization identity; otherwise, the result code 123 is returned.

## 4. Implementation Considerations

One possible interaction of proxy authorization and normal access control is illustrated here. During evaluation of a search request, an entry that would have been returned for the search (if submitted by the proxy authorization identity directly) may not be returned if

the server finds that the requester does not have the right to assume the requested identity for searching the entry, even if the entry is within the scope of a search request under a base DN that does imply such rights. This means that fewer results, or no results, may be returned than would be if the proxy authorization identity issued the request directly. An example of such a case may be a system with fine-grained access control, where the proxy right requester has proxy rights at the top of a search tree, but not at or below a point or points within the tree.

## 5. Security Considerations

The Proxy Authorization Control method is subject to general LDAP security considerations [RFC2251] [AUTH] [LDAPTLS]. The control may be passed over a secure channel as well as over an insecure channel.

The control allows for an additional authorization identity to be passed. In some deployments, these identities may contain confidential information that requires privacy protection.

Note that the server is responsible for determining if a proxy authorization request is to be honored. "Anonymous" users SHOULD NOT be allowed to assume the identity of others.

## 6. IANA Considerations

The OID "2.16.840.1.113730.3.4.18" is reserved for the Proxy Authorization Control. It has been registered as an LDAP Protocol Mechanism [RFC3383].

A result code (123) has been assigned by the IANA for the case where the server does not execute a request using the proxy authorization identity.

## 7. Acknowledgements

Mark Smith, formerly of Netscape Communications Corp., Mark Wahl, formerly of Sun Microsystems, Inc., Kurt Zeilenga of OpenLDAP Foundation, Jim Sermersheim of Novell, and Steven Legg of Adacel have contributed with reviews of this document.

## 8. Normative References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[LDAPV3] Hodges, J. and R. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002.

[SASL] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222, October 1997.

[AUTH] Wahl, M., Alvestrand, H., Hodges, J., and R. Morgan, "Authentication Methods for LDAP", RFC 2829, May 2000.

[LDAPTLS] Hodges, J., Morgan, R., and M. Wahl, "Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security", RFC 2830, May 2000.

[RFC2251] Wahl, M., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[RFC2252] Wahl, M., Coulbeck, A., Howes, T., and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997.

[RFC2829] Wahl, M., Alvestrand, H., Hodges, J., and R. Morgan, "Authentication Methods for LDAP", RFC 2829, May 2000.

[RFC3383] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", BCP 64, RFC 3383, September 2002.

## Author's Address

Rob Weltman
Yahoo!, Inc.
701 First Avenue
Sunnyvale, CA 94089
USA

Phone: +1 408 349-5504
EMail: robw@worldspot.com

## Full Copyright Statement

Copyright (C) The Internet Society (2006).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

## Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

## Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).