Network Working Group
Request for Comments: 4522
Category: Standards Track

S. Legg
eB2Bcom

June 2006

Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option

Status of This Memo

Copyright Notice

Abstract

Each attribute stored in a Lightweight Directory Access Protocol (LDAP) directory has a defined syntax (i.e., data type). A syntax definition specifies how attribute values conforming to the syntax are normally represented when transferred in LDAP operations. This representation is referred to as the LDAP-specific encoding to distinguish it from other methods of encoding attribute values. This document defines an attribute option, the binary option, that can be used to specify that the associated attribute values are instead encoded according to the Basic Encoding Rules (BER) used by X.500 directories.

Table of Contents

1. Introduction

Each attribute stored in a Lightweight Directory Access Protocol (LDAP) directory [RFC4510] has a defined syntax (i.e., data type) which constrains the structure and format of its values.

The description of each syntax [RFC4517] specifies how attribute or assertion values [RFC4512] conforming to the syntax are normally represented when transferred in LDAP operations [RFC4511]. This representation is referred to as the LDAP-specific encoding to distinguish it from other methods of encoding attribute values.

This document defines an attribute option, the binary option, which can be used in an attribute description [RFC4512] in an LDAP operation to specify that the associated attribute values or assertion values are, or are requested to be, encoded according to the Basic Encoding Rules (BER) [BER] as used by X.500 [X.500] directories, instead of the usual LDAP-specific encoding.

The binary option was originally defined in RFC 2251 [RFC2251]. The LDAP technical specification [RFC4510] has obsoleted the previously defined LDAP technical specification [RFC3377], which included RFC 2251. The binary option was not included in the revised LDAP technical specification for a variety of reasons including implementation inconsistencies. No attempt is made here to resolve the known inconsistencies.

This document reintroduces the binary option for use with certain attribute syntaxes, such as certificate syntax [RFC4523], that specifically require it. No attempt has been made to address use of the binary option with attributes of syntaxes that do not require its use. Unless addressed in a future specification, this use is to be avoided.

2. Conventions

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 BCP 14, RFC 2119 [BCP14].

3. The Binary Option

The binary option is indicated with the attribute option string "binary" in an attribute description. Note that, like all attribute options, the string representing the binary option is case insensitive.

Where the binary option is present in an attribute description, the associated attribute values or assertion values MUST be BER encoded (otherwise the values are encoded according to the LDAP-specific encoding [RFC4517] for the attribute's syntax). Note that it is possible for a syntax to be defined such that its LDAP-specific encoding is exactly the same as its BER encoding.

In terms of the protocol [RFC4511], the binary option specifies that the contents octets of the associated AttributeValue or AssertionValue OCTET STRING are a complete BER encoding of the relevant value.

The binary option is not a tagging option [RFC4512], so the presence of the binary option does not specify an attribute subtype. An attribute description containing the binary option references exactly the same attribute as the attribute description without the binary option. The supertype/subtype relationships of attributes with tagging options are not altered in any way by the presence or absence of the binary option.

An attribute description SHALL be treated as unrecognized if it contains the binary option and the syntax of the attribute does not have an associated ASN.1 type [RFC4517], or the BER encoding of values of that type is not supported.

The presence or absence of the binary option only affects the transfer of attribute and assertion values in the protocol; servers store any particular attribute value in a format of their choosing.

4. Syntaxes Requiring Binary Transfer

The attribute values of certain attribute syntaxes are defined without an LDAP-specific encoding and are required to be transferred in the BER-encoded form. For the purposes of this document, these syntaxes are said to have a binary transfer requirement. The certificate, certificate list, certificate pair, and supported algorithm syntaxes [RFC4523] are examples of syntaxes with a binary transfer requirement. These syntaxes also have an additional requirement that the exact BER encoding must be preserved. Note that this is a property of the syntaxes themselves, and not a property of the binary option. In the absence of this requirement, LDAP clients would need to re-encode values using the Distinguished Encoding Rules (DER).

5. Attributes Returned in a Search

An LDAP search request [RFC4511] contains a list of the attributes (the requested attributes list) to be returned from each entry matching the search filter. An attribute description in the requested attributes list also implicitly requests all subtypes of the attribute type in the attribute description, whether through attribute subtyping or attribute tagging option subtyping [RFC4512].

The requested attributes list MAY contain attribute descriptions with the binary option, but MUST NOT contain two attribute descriptions with the same attribute type and the same tagging options (even if only one of them has the binary option). The binary option in an attribute description in the requested attributes list implicitly applies to all the subtypes of the attribute type in the attribute description (however, see Section 7).

Attributes of a syntax with the binary transfer requirement, if returned, SHALL be returned in the binary form (i.e., with the binary option in the attribute description and the associated attribute values BER encoded) regardless of whether the binary option was present in the request (for the attribute or for one of its supertypes).

Attributes of a syntax without the binary transfer requirement, if returned, SHOULD be returned in the form explicitly requested. That is, if the attribute description in the requested attributes list contains the binary option, then the corresponding attribute in the result SHOULD be in the binary form. If the attribute description in the request does not contain the binary option, then the corresponding attribute in the result SHOULD NOT be in the binary form. A server MAY omit an attribute from the result if it does not support the requested encoding.

Regardless of the encoding chosen, a particular attribute value is returned at most once.

6. All User Attributes

If the list of attributes in a search request is empty or contains the special attribute description string "*", then all user attributes are requested to be returned.

Attributes of a syntax with the binary transfer requirement, if returned, SHALL be returned in the binary form.

Attributes of a syntax without the binary transfer requirement and having a defined LDAP-specific encoding SHOULD NOT be returned in the binary form.

Attributes of a syntax without the binary transfer requirement and without a defined LDAP-specific encoding may be returned in the binary form or omitted from the result.

7. Conflicting Requests

A particular attribute could be explicitly requested by an attribute description and/or implicitly requested by the attribute descriptions of one or more of its supertypes, or by the special attribute description string "*". If the binary option is present in at least one, but not all, of these attribute descriptions then the effect of the request with respect to binary transfer is implementation defined.

8. Security Considerations

When interpreting security-sensitive fields, and in particular fields used to grant or deny access, implementations MUST ensure that any matching rule comparisons are done on the underlying abstract value, regardless of the particular encoding used.

9. IANA Considerations

The Internet Assigned Numbers Authority (IANA) has updated the LDAP attribute description option registry [BCP64] as indicated by the following template:

```
Subject:
  Request for LDAP Attribute Description Option Registration
Option Name: binary
Family of Options: NO
Person & email address to contact for further information:
  Steven Legg <steven.legg@eb2bcom.com>
Specification: RFC 4522
Author/Change Controller: IESG
```

10. References

10.1. Normative References

[BCP14] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[BCP64] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", BCP 64, RFC 4520, June 2006.

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC RFC 4510, June 2006.

[RFC4511] Sermersheim, J., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, June 2006.

[RFC4512] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

[RFC4517] Legg, S., Ed., "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules", RFC 4517, June 2006.

[RFC4523] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates", RFC 4523, June 2006.

[BER] ITU-T Recommendation X.690 (07/02) | ISO/IEC 8825-1, Information Technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

10.2. Informative References

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

[RFC3377] Hodges, J. and R. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002.

[X.500] ITU-T Recommendation X.500 (02/01) | ISO/IEC 9594-1:2001, Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services

Author's Address

Dr. Steven Legg
eB2Bcom
Suite 3, Woodhouse Corporate Centre
935 Station Street
Box Hill North, Victoria 3129
AUSTRALIA

Phone: +61 3 9896 7830
Fax: +61 3 9896 7801
EMail: steven.legg@eb2bcom.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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