Internet X.509 Public Key Infrastructure
Operational Protocols - LDAPv3
<draft-ietf-pkix-ldap-v3-05.txt>

STATUS OF THIS MEMO

This Internet-Draft expires on 5 July 2002.

Comments and suggestions on this document are encouraged. Comments on this document should be sent to the PKIX working group discussion list:

<ietf-pkix@imc.org>

or directly to the author.

ABSTRACT

This document describes the features of the Lightweight Directory Access Protocol v3 that are needed in order to support a public key infrastructure based on X.509 certificates and CRLs.

1. Introduction

RFC 2559 [1] specifies the subset of LDAPv2 [2] that is necessary to retrieve X.509 [9] certificates and CRLs from LDAP servers. However LDAPv2 has a number of deficiencies that may limit its usefulness in certain circumstances. The most notable of these are:

- LDAPv2 distinguished names must be composed from the IA5 character set and cannot contain accented or non-latin characters,

- LDAPv2 only has a limited number of supported authentication schemes for binding to the server, in particular the use of hashed passwords or TLS [3] are not supported,

- LDAPv2 only supports a single directory server. It is the responsibility of the user to pre-configure his client with the required set of LDAP servers, and to choose the correct one for each certificate and CRL retrieval.

It is for these reasons (and others not listed here) that the IETF have stopped the standardisation of the LDAPv2 protocol and have replaced it with the LDAPv3 protocol [4]. However the LDAPv3 protocol is much more complex than the LDAPv2 protocol and many of its features are not essential for simple PKIX use. This document describes the features of LDAPv3 that are essential, or not required, or are optional for servers to support a PKI based on X.509.

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 RFC 2119 [5].

2. Model

The PKI components, as defined in RFC 2510 [16], which are involved in PKIX operational protocol interactions include:

- End Entities
- Certification Authorities (CA)
- Repository

End entities and CAs using LDAPv3, retrieve PKI information from the repository using a subset of the LDAPv3 protocol. Where the retrieving entity has knowledge of the distinguished name of the LDAP entry being sought, a "repository read" may be performed. Where the distinguished name of the LDAP entry is not known, but some other related information is known, a "repository search" is performed for candidate entries.

CAs populate the repository with PKI information using a subset of the LDAPv3 protocol. CAs may add, delete and modify PKI information in the repository using "repository modify" operations.

3. LDAPv3 Operations

A repository read is performed using an LDAPv3 SearchRequest operation, where the filter is set to present with an attribute type of object class, the scope is set to baseObject, and the base object is set to the distinguished name of the entry.

A repository search is performed for candidate entries using an LDAPv3 SearchRequest operation where the filter is set to information related to the LDAP entry being sought, and the base object is set to the distinguished name of any entry, including null (but is typically set to the name of an entry superior in the DIT to the entry being sought). Scope may be set to any of the three values, but is typically set to wholeSubtree.

BindRequests may or may not be sent prior to SearchRequest operations (see later).

Repository modifies may be performed using an LDAPv3 AddRequest operation to add a new entry to the LDAP repository, an LDAPv3 DelRequest to delete an existing entry from the LDAP repository, and an LDAPv3 ModifyRequest to update the contents of an entry. Repository modifies must be preceded by BindRequests to provide an adequate level of authentication (see later).

No other LDAP operations are required by this profile.

4. Features Of Ldapv3 That MUST Be Supported

Attribute descriptions are a superset of attribute type definitions. They allow attribute subtyping to be specified in the LDAPv3 protocol. The ;binary option is an exception to this. This option allows certificates and CRLs to be asked for and returned as binary values encoded using the Basic Encoding Rules [11]. The mechanism described in RFC2559 (PKIX LDAPv2) [1] is fully compliant with the ;binary option of LDAPv3. The ;binary option of attribute descriptions MUST be supported by all implementations. When a client adds, deletes, retrieves or modifies attribute values that are defined in RFC 2256 [13] to be stored and requested in the binary form, the attribute type name MUST always be specified with the ;binary attribute option. When the server returns such an attribute in a search result, the attribute type name MUST include the ;binary option. Other attribute description options SHOULD NOT be generated by clients. Servers MAY choose to support them at their discretion.

UTF8 encoding [12] allows the full ISO 10646 character set to be used in the creation of distinguished names. UTF8 encoding of distinguished names MUST be supported as specified in RFC2253 [6].

Multiple attribute value assertions (AVAs) within RDN components of distinguished names MUST be supported and the ordering of the AVAs is non-deterministic. For example cn=John + serialNumber=123 is the same as serialNumber=123 + cn=John.

LDAPv3 has the concept of unsolicited notifications that can be sent from the server to the client. This is used to indicate when the server is going down, so that a client can distinguish between a server failure and a network failure. A client MUST be prepared to accept unsolicited notifications defined in RFC 2251 [4].

The altServer attribute is used by servers to point to alternative servers that may be contacted if this server is temporarily unavailable. This attribute MUST be stored in the root DSE of the server and MUST be available to clients for retrieval. (The access controls on this attribute MUST be the same or less than those on certificates and revocation lists.) If no alternative servers exist this attribute MUST point to the current server. Clients MAY make use of this feature but do not need to. Servers MAY store any other operational attributes in the root DSE, but do not need to, except where mandated in this or other profiles.

If the Certification Practice Statement (CPS) allows unauthenticated anonymous access to the server, then the server MUST allow a client to perform a SearchRequest operation (for a repository read or repository search type request) without issuing a prior Bind operation. The server MUST also allow the client to present a Bind request with the simple authentication choice and a zero-length OCTET STRING.

If the CPS allows weak password based authentication for repository read or repository search access to the server, the client and the server MUST support the DIGEST-MD5 mechanism [7] as specified in [8] and [10].

5. Features Of Ldapv3 That SHOULD Be Supported

In a distributed directory with multiple servers, LDAPv3 supports referrals as the mechanism to allow one server that cannot fulfil a client's request, to refer the client to another server that might be better able to fulfil the request. Servers SHOULD be able to return referrals to clients. Clients SHOULD be able to receive referrals and process them, although they are not required to automatically process them and support multiple asynchronous outgoing connections.

Partial Search results are returned when a server only has a subset of the certificates requested by the client. Referrals to other servers are embedded in the SearchResultReference field. Clients and servers SHOULD be able to handle SearchResultReferences in the same way as they handle referrals.

However, the returned referrals SHOULD NOT specify new search filters, attributes to be returned or user credentials. Servers SHOULD only return the hostport and DN components and MAY return the scope component.

6. Features Of Ldapv3 that are Not Used by this Profile

A client following this profile need not send the ModifyDN, Compare and Abandon operations. The server MAY choose to support these operations at its discretion. (Note that a client wishing to abnormally terminate a search request may, instead of issuing an Abandon operation, close the TCP/IP connection.)

The LDAPv3 protocol is infinitely extensible via two mechanisms: extended operations and controls on existing operations. The client does not need to generate any LDAPv3 protocol extensions (extended operations or controls), unless flexible searching for certificates is supported (see below). The server SHOULD NOT return any LDAPv3 protocol extensions (extended operations or controls) apart from those necessary to support the controls already used by the client.

7. Features Of Ldapv3 That MAY Be Supported

The default behaviour for LDAPv3 servers is that a user must retrieve all the attribute values from an attribute, or none of them (subject of course to having access rights to the values). If the user of an LDAPv3 server wishes to retrieve a limited number of attribute values, specifically those that match certain filtering criteria, (for example a data encryption userCertificate from a user's entry, or a revocation list that was current at a particular moment in time) then this MAY be achieved by using the LDAPv3 valuesReturnFilter control [15] along with the certificateExactMatch, certificateMatch, certificateListExactMatch or certificateListMatch matching rules [14].

If the CPS allows weak password based authentication for "read" or "search" access to the server, the client and the server MAY support a simple password Bind sequence following the negotiation of a TLS ciphersuite to provide connection confidentiality, as specified in [10].

If the CPS requires strong authentication for access to the server then the client and the server SHOULD support certificate based authentication as specified in [10].

8. Security Considerations

The PKI information to be retrieved from LDAPv3 servers (certificates and CRLs) is digitally signed and therefore additional integrity services are NOT REQUIRED. However, clients that retrieve CRLs without some way of verifying the server run the risk of being sent a still current but superceded CRL.

The CPS will specify whether the information should be publicly available or not. If publicly available, privacy services will NOT be REQUIRED for retrieval requests. If not publicly available, privacy services MAY be REQUIRED and these can be provided by a TLS ciphersuite as specified in clause 5.

For update of the information by CAs either strong authentication or weaker password based authentication MUST be supported as specified in clause 5. Additional access controls SHOULD be provided.

Organizations are NOT REQUIRED to provide external CAs or users with access to their directories.

9. Copyright

10. References

[1] S.Boeyen, T. Howes, P. Richard "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2", RFC 2559, April 1999
[2] Yeong, W., Howes, T., and Kille, S. "Lightweight Directory Access Protocol", RFC 1777, March 1995.
[3] T. Dierks, C. Allen. "The TLS Protocol Version 1.0", RFC 2246, January 1999.
[4] M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3)", Dec. 1997, RFC 2251
[5] S.Bradner. "Key words for use in RFCs to Indicate Requirement

Levels", RFC 2119, March 1997.
[6] M. Wahl, S. Kille, T. Howes. "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC2253, December 1997.
[7] R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992
[8] P. Leach, C. Newman, "Using Digest Authentication as a SASL Mechanism", RFC 2831, May 2000.
[9] ITU-T Rec. X.509(97) The Directory: Authentication Framework
[10] M. Wahl, H. Alvestrand, J. Hodges, R. Morgan. "Authentication Methods for LDAP", RFC 2829, May 2000
[11] ITU-T Rec. X.690, "Specification of ASN.1 encoding rules: Basic, Canonical, and Distinguished Encoding Rules", 1994.
[12] F. Yergeau. "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.
[13] M.Wahl. "A Summary of the X.500(96) User Schema for use with LDAPv3" RFC 2256, Dec 1997
[14] D.W.Chadwick, S.Legg. "Internet X.509 Public Key Infrastructure - LDAP Schema and Syntaxes for PKIs and PMIs", <draft-pkix-ldap-schema-02.txt>, November 2001
[15] D.Chadwick, S.Mullan. "Returning Matched Values with LDAPv3", Internet Draft <draft-ldapext-matchedval-05.txt>, December 2000
[16] Adams, C., Farrell, S., "Internet X.509 Public Key Infrastructure Certificate Management Protocols," RFC 2510, March 1999.

11. Authors Address

David Chadwick
IS Institute
University of Salford
Salford
England
M5 4WT

Email: d.w.chadwick@salford.ac.uk

12. Document History

Changes Made to Version 01

i) Schema removed to a separate document
ii) Selecting individual attribute values updated to reflect new LDAP Internet Draft
iii) Re-wording of text surrounding the use of ;binary option.

Changes Made to Version 02

i) Added text to Security section about superceded CRLs.
ii) Changed text in section 4 about which controls server can send to client
iii) Updated references section
iv) Added selective retrieving of CRLs to section 5

Changes Made to Version 03

i) Updated references only.

Changes Made to Version 04

i) Removed reference to RFC 2559 from all but the introduction to this document and copied relevant text from it into the body of this document, so that the reader will not need to reference RFC2559 when implementing this RFC. (Note that not all of RFC2559 has been copied as some of it has been superseded, and some of it now seems to be unnecessary e.g. mandating time limit of zero be supported).