Internet-Draft
PKIX WG
Intended Category: Standards Track
Expires: 8 October 2002

David Chadwick
University of Salford

8 April 2002

LDAPv3 DN strings for use with PKIs
<draft-ietf-pkix-dnstrings-00.txt>

STATUS OF THIS MEMO

This Internet-Draft expires on 8 October 2002.

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

ietf-pkix@imc.org

or directly to the authors.

ABSTRACT

RFC 2253 [2] standardises a set of strings that can be used to represent attribute types in LDAP distinguished names. This list is does not cover the full set of attribute types used in the distinguished names of issuers and subjects in public key certificates. This document standardises the strings needed for these additional attribute types.

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 [3].

1. Introduction

RFC 2253 standardises a set of strings for a limited number of attribute types that can be used in the LDAP encoding of X.500 distinguished names. These are

String	X.500 AttributeType
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

The revision of RFC 2253 [5] states that additional attribute types should be represented by their object identifiers.

RFC 3039 [4] lists the following attribute types that may be used to create subject and issuer distinguished names:

countryName;
commonName;
surname;
givenName;
pseudonym;
serialNumber;
organizationName;
organizationalUnitName;
stateOrProvinceName
localityName and
postalAddress.

The observant reader will notice that the serialNumber, pseudonym, and postalAddress attribute types are missing from the RFC 2253 set and consequently do not have standardised strings for use in LDAP distinguished names.

Other examples are... [to be added by members of the PKIX group]

2. Additional LDAP String Definitions

This document defines the following additional strings that SHOULD be used to represent their respective attribute types in LDAP distinguished names, as given in the following table:

String	X.500 AttributeType
serialNumber	serialNumber
ADDR	postalAddress
Pseudo	pseudonym

[other strings to be added by members of PKIX group]

Note. The strings are case insensitive as far as LDAPv3 is concerned

3. Security Considerations

The following security considerations are specific to the handling of distinguished names. LDAP security considerations are discussed in [6] and other documents comprising the LDAP Technical Specification [7].

4. Acknowledgements

None at present

5. Copyright

6. References

[1] S. Bradner. "The Internet Standards Process -- Revision 3", RFC 2026, October 1996.
[2] Wahl, M., Kille, S., Howes, T. "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC2253, December 1997.
[3] S.Bradner. "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.
[4] Santesson,S., Polk, W., Barzin, P., Nystrom, M. "Internet X.509 Public Key Infrastructure Qualified Certificates Profile", RFC 3039, Jan 2001
[5] K. Zeilenga. "LDAP: String Representation of Distinguished Names". <draft-ietf-ldapbis-dn-07.txt>,1 March 2002
[6] J. Sermersheim (editor), "LDAP: The Protocol", <draft-ietf-ldapbis-protocol-xx.txt>, a work in progress.
[7] K. Zeilenga (editor), "LDAP: Technical Specification Road Map", <draft-ietf-ldapbis-roadmap-xx.txt>, a work in progress.

7. Authors Address

David Chadwick
IS Institute
University of Salford
Salford M5 4WT

England

Email: d.w.chadwick@salford.ac.uk
Tel: +44 161 295 5351