Network Working Group S. Leonard
Internet-Draft Penango, Inc.
Intended Status: Informational November 14, 2017
Expires: May 18, 2018

Lightweight Directory Access Protocol (LDAP) Registrations for PKCS #9 draft-seantek-ldap-pkcs9-08

Abstract

PKCS #9 includes several useful definitions that are not yet reflected in the LDAP IANA registry. This document adds those definitions to the IANA registry.

Status of This Memo

Copyright Notice

1. Introduction

This document registers the LDAP [LDAPMAP] schema definitions [LDAPDIM] for a subset of elements specified in PKCS #9 [PKCS#9], including attribute types; matching rules and syntaxes to be used with these attribute types; and related object classes.

The Public Key Cryptography Standard (PKCS) series is a group of documents originally published by RSA Security, Inc. in the early 1990s. These de-facto industry standards specify cryptographic formats and associated operations, such as the mathematical properties of the RSA algorithm and of cryptographic software and hardware modules. Since initial publication, change control of many PKCS documents was transferred to the IETF.

[PKCS#9] "Selected Object Classes and Attribute Types" "provides a selection of object classes and attribute types for use in conjunction with public-key cryptography and Lightweight Directory Access Protocol (LDAP) accessible directories." Many of these ASN.1 data items are used throughout cryptographic implementations, but standardized names were never put into the IANA LDAP Parameters registry. LDAP parameters are frequently user-visible (for better or for worse) so registering these parameters will improve both interoperability and usability.

As the elements and their semantics are defined in [PKCS#9], this document needs to be read in conjunction with [PKCS#9] to make use of the LDAP registrations provided herein. [PKCS#9] provides complete definitions, with one significant omission: the IANA Considerations section was never appended. This document provides the IANA Considerations section necessary to register appropriate descriptors.

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 [BCP14].

2. Syntaxes

Appendix B.1 of [PKCS#9] describes various syntaxes used in LDAP to transfer PKCS #9 elements and related data types.

3. Matching Rules

Appendix B.4 of [PKCS#9] provides matching rules for use in LDAP.

4. Attribute Types

Appendix B.3 of [PKCS#9] details attribute types for use in LDAP,

including (by its own admission) attributes that are "highly unlikely" to be stored in a Directory. This document registers all such attributes en masse.

[PKCS#9] includes certain attribute types that have found meaningful use outside of the PKCS series. Specifically:

- emailAddress is mandated in [SMIMEv3.2C], and has mandatory processing requirements if included in a certificate [PKIXPROF].
- [PKIXPROF] recommends the recognition of pseudonym.
- The Qualified Certificates Profile [QCPROF] requires both pseudonym and the vital records dateOfBirth, placeOfBirth, gender, countryOfCitizenship, and countryOfResidence.
- "DESC" is sometimes emitted for the description (2.5.4.13) attribute.

As a result, certain applications not only encounter and generate these attributes in practice, but also use short descriptors that have come to be widely recognized.

Implementations SHOULD also note that "gn" is a common descriptor for "givenName" (2.5.4.42), and is widely emitted by cryptographic applications.

4.1. Semantics of dateOfBirth Clarified

[PKCS#9] Section 5.2.4 states that dateOfBirth "is the date of birth for the subject it is associated with." Its GeneralizedTime syntax, however, requires time and time zone specifications that are not related to dateOfBirth's semantics.

[QCPROF] RECOMMENDS that the time recorded be GMT (i.e., UTC) noon down to the granularity of seconds "in order to prevent accidental change of date due to time zone adjustments." Since contemporary time zones range from -1200 to +1400, however, naive processing will misinterpret this value by one day for timezones significantly ahead of UTC.

The semantics of dateOfBirth are hereby defined: in dateOfBirth, only the date is meaningful. Parsers that need to convert the GeneralizedTime value to a specific point in time MUST decode the date in the UTC timezone to avoid shifting of the date due to timezone differences (such as in +14). Thus, a subject born in GMT+1400 will have a GeneralizedTime value that is essentially one day ahead (2am), when interpreted literally.

When stored in LDAP, a conformant implementation MAY record this

value in UTC or in local time, but MUST NOT record this value with a timezone offset. I.e., [X.680] subclauses 46.2 a) and b) and 46.3 a) and b) are acceptable; subclauses 46.2 c) and 46.3 c) are not acceptable. When comparing such values, "local time" values SHALL be compared as if the local time is UTC.

The following sentence of [QCPROF] Section 3.2.2 remains in effect for both certificate and non-certificate uses: "Compliant [certificate] [sic] parsing applications SHOULD ignore any time data and just present the contained date without any time zone adjustments."

4.2. Short Descriptors for Certain Useful Attribute Types

As permitted by Section 3.4 of [LDAPIANA], the short descriptors in Table 1 are registered along with their more verbose counterparts reflected in [PKCS#9]:

Short Descriptor	Regular Descriptor
e	emailAddress
dob	dateOfBirth
pob	placeOfBirth
g	gender
coc	countryOfCitizenship
cor	countryOfResidence
pnym	pseudonym

Table 1: Short Descriptors for Certain Attribute Types

4.3. Short Descriptors for Certain Other Attribute Types

As permitted by Section 3.4 of [LDAPIANA], the short descriptors in Table 2 are registered along with their more verbose counterparts elsewhere:

Short Descriptor	Regular Descriptor
desc	description

Table 2: Short Descriptors for Certain Attribute Types

5. Object Classes

Appendix B.2 of [PKCS#9] details a set of object classes for use in LDAP.

6. Security Considerations

PKCS #9 security considerations (written for the RFC edition) [PKCS#9] apply to the definitions in this document. LDAP security and privacy considerations in [LDAPMAP] and [LDAPDIM] apply as well.

Some attributes such as those in [QCPROF], namely dateOfBirth, placeOfBirth, gender, countryOfCitizenship, and countryOfResidence are sensitive and may be subject to privacy laws in certain jurisdictions. If conveyed with LDAP, these attributes ought to be returned over a protected channel, such as TLS.

7. IANA Considerations

The IANA shall register an LDAP Object Identifier [LDAPIANA] for use in this technical specification. The IANA shall update the LDAP Descriptor registry [LDAPIANA] with definitions from [PKCS#9] as indicated below.

7.1. Object Identifier Registration

Subject: Request for LDAP OID Registration
Person & email address to contact for further information:
Sean Leonard <dev+ietf@seantek.com>
Specification: draft-seantek-ldap-pkcs9
Author/Change Controller: IESG
Comments:
Identifies the PKCS #9 schema elements registered in the IANA LDAP Descriptor and Syntaxes registries via this document.

7.2. Descriptor Registration

Subject: Request for LDAP Descriptor Registration
Descriptor (short name): see table
Object Identifier: see table
Person & email address to contact for further information:
Sean Leonard <dev+ietf@seantek.com>
Usage: see table
Specification: draft-seantek-ldap-pkcs9
Author/Change Controller: IESG

pkcsEntity	O	1.2.840.113549.1.9.24.1
naturalPerson	O	1.2.840.113549.1.9.24.2
pKCS7PDU	A	1.2.840.113549.1.9.25.5
userPKCS12	A	2.16.840.1.113730.3.1.216
pKCS15Token	A	1.2.840.113549.1.9.25.1
encryptedPrivateKeyInfo	A	1.2.840.113549.1.9.25.2

e	A	1.2.840.113549.1.9.1
unstructuredName	A	1.2.840.113549.1.9.2
unstructuredAddress	A	1.2.840.113549.1.9.8
dob	A	1.3.6.1.5.5.7.9.1
dateOfBirth	A	1.3.6.1.5.5.7.9.1
pob	A	1.3.6.1.5.5.7.9.2
placeOfBirth	A	1.3.6.1.5.5.7.9.2
g	A	1.3.6.1.5.5.7.9.3
gender	A	1.3.6.1.5.5.7.9.3
coc	A	1.3.6.1.5.5.7.9.4
countryOfCitizenship	A	1.3.6.1.5.5.7.9.4
cor	A	1.3.6.1.5.5.7.9.5
countryOfResidence	A	1.3.6.1.5.5.7.9.5
pnym	A	2.5.4.65
desc	A	2.5.4.13

Add a note to the following attributes:
This attribute is to be used in PKCS applications
(including PKCS #6, PKCS #7/CMS, and PKCS #12).

contentType	A	1.2.840.113549.1.9.3
messageDigest	A	1.2.840.113549.1.9.4
signingTime	A	1.2.840.113549.1.9.5
randomNonce	A	1.2.840.113549.1.9.25.3
sequenceNumber	A	1.2.840.113549.1.9.25.4
counterSignature	A	1.2.840.113549.1.9.6
challengePassword	A	1.2.840.113549.1.9.7
extensionRequest	A	1.2.840.113549.1.9.14
extendedCertificateAttributes	A*	1.2.840.113549.1.9.9
friendlyName	A	1.2.840.113549.1.9.20
localKeyId	A	1.2.840.113549.1.9.21
signingDescription	A	1.2.840.113549.1.9.13
smimeCapabilities	A	1.2.840.113549.1.9.15
pkcs9CaseIgnoreMatch	M	1.2.840.113549.1.9.27.1
signingTimeMatch	M	1.2.840.113549.1.9.27.3

7.3. PKCS9String Syntax Registration

Subject: Request for LDAP Syntax Registration
Object Identifier: 1.2.840.113549.1.9.26.1
Description: PKCS9String
Person & email address to contact for further information:
    Sean Leonard <dev+ietf@seantek.com>
Specification: draft-seantek-ldap-pkcs9
Author/Change Controller: IESG
Comments:
     Identifies the PKCS #9 String syntax, which is
     a CHOICE of IA5String and DirectoryString.

7.4. SigningTime Syntax Registration

Subject: Request for LDAP Syntax Registration
Object Identifier: 1.2.840.113549.1.9.26.2
Description: SigningTIme
Person & email address to contact for further information:
    Sean Leonard <dev+ietf@seantek.com>
Specification: draft-seantek-ldap-pkcs9
Author/Change Controller: IESG
Comments:
     Identifies the SigningTime syntax, which is Time,
     which is a CHOICE of UTCTime and GeneralizedTime.

8. Acknowledgements

This document relies on PKCS #9, a product of RSA Laboratories.

9. References

9.1. Normative References

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

[PKCS#9] Nystrom, M. and Kaliski, B., "PKCS #9: Selected Object Classes and Attribute Types Version 2.0", RFC 2985, November 2000.

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

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

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

[X.680] International Telecommunication Union, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1, August 2015.

9.2. Informative References

[QCPROF] Santesson, S., Nystrom, M., and T. Polk, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 3739, March 2004.

[PKIXPROF] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[SMIMEv3.2C] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling", RFC 5750, January 2010.

Author's Address

Sean Leonard
Penango, Inc.
5900 Wilshire Blvd
Ste 2600
Los Angeles, CA 90036
USA

EMail: dev+ietf@seantek.com
URI: http://www.penango.com/