Network Working Group
Internet-Draft
Intended Status: Informational
Expires: March 14, 2015

S. Leonard
Penango, Inc.

September 10, 2014

Lightweight Directory Access Protocol (LDAP) Registrations for PKCS #9 draft-seantek-ldap-pkcs9-00.txt

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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 14, 2015.

Copyright Notice

1. Introduction

This document registers the LDAP [RFC4510] schema definitions [RFC4512] for a subset of elements specified in PKCS #9 [PKCS9], including attribute types; matching rules and syntaxes to be used with these attribute types; and related object classes.

As the elements and their semantics are defined in [PKCS9], this document needs to be read in conjunction with [PKCS9] to make use of the LDAP registrations provided herein. [PKCS9] 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.

2. Syntaxes

Appendix B.1 of [PKCS9] describes various syntaxes used in LDAP to transfer PKCS #9 elements and related data types.

3. Matching Rules

Appendix B.4 of [PKCS9] provides matching rules for use in LDAP.

4. Attribute Types

Appendix B.3 of [PKCS9] details attribute types for use in LDAP, including (by its own admission) attributes that are highly unlikely to be stored in a Directory. For parity, all attributes in Appendix B.3--but not necessarily in PKCS #9 as a whole--are registered via this document.

4.1 Short Descriptors for Certain Useful Attribute Types

[PKCS9] includes certain attribute types that have found meaningful use outside of the PKCS series. Specifically:

- emailAddress is mandated in [RFC5750], and has mandatory processing requirements if included in a certificate [RFC5280].
- [RFC5280] recommends the recognition of pseudonym.
- The Qualified Certificates Profile [RFC3739] requires both pseudonym and the vital records dateOfBirth, placeOfBirth, gender, countryOfCitizenship, and countryOfResidence.

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.

As permitted by Section 3.4 of [RFC4520], the short descriptors in

Table 1 are registered along with their more verbose counterparts reflected in [PKCS9]:

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

5. Object Classes

Appendix B.2 of [PKCS9] details a set of object classes for use in LDAP.

6. Security Considerations

PKCS #9 security considerations (written for the RFC edition) [PKCS9] apply to the definitions in this document. General LDAP security considerations [RFC4510] apply as well.

7. IANA Considerations

The IANA shall register an LDAP Object Identifier [RFC4520] for use in this technical specification, and shall update the LDAP Descriptor registry [RFC4520], 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
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
counterSignature	A	1.2.840.113549.1.9.6
challengePassword	A	1.2.840.113549.1.9.7
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

[PKCS9] Nystrom, M. and Kaliski, B., "PKCS #9: Selected Object Classes and Attribute Types Version 2.0", RFC 2985, November 2000.

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

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

[RFC4520] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access

Protocol (LDAP)", BCP 64, RFC 4520, June 2006.

9.2. Informative References

[RFC3739] Santesson, S., Nystrom, M., and T. Polk, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", RFC 3739, March 2004.

[RFC5280] 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.

[RFC5750] 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 Boulevard
21st Floor
Los Angeles, CA 90036
USA

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