Curdle
Internet-Draft
Intended status: Informational
Expires: July 29, 2018

J. Schaad
August Cellars
R. Andrews
DigiCert, Inc.

January 25, 2018

IANA Registration for new Cryptographic Algorithm Object Identifier Range
draft-schaad-curdle-oid-registry-03

Abstract

When the Curdle Security Working Group was chartered, a range of object identifiers was donated by DigiCert, Inc. for the purpose of registering the Edwards Elliptic Curve key agreement and signature algorithms. This donated set of OIDs allowed for shorter values than would be possible using the existing S/MIME or PKIX arcs. This document describes the range of identifiers that were assigned in that donated range, transfers control of that range to IANA, and establishes IANA allocation policies for any future assignments within that range.

Contributing to this document

The source for this draft is being maintained in GitHub. Suggested changes should be submitted as pull requests at <https://github.com/lamps-wg/smime>. Instructions are on that page as well. Editorial changes can be managed in GitHub, but any substantial issues need to be discussed on the LAMPS mailing list.

Table of Contents

1. Introduction 2
2. IANA Considerations 3
2.1. "SMI Security for Cryptographic Algorithms" Registry . . 3
3. Security Considerations 4
4. References 4
4.1. Normative References 4
4.2. Informational References 4
Acknowledgments 5
Authors' Addresses 5

1. Introduction

When the Curdle Security Working Group was chartered, a range of object identifiers was donated by DigiCert, Inc. for use by that working group. The use of these object identifiers allowed for the Edwards Ellitptic Curve key agreement [RFC7748] and signature [RFC8032] algorithms to be defined with encodings that are smaller than similar ones would be if assigned from the existing S/MIME or PKIX arcs. These initial registrations from this arc were done while developing [I-D.ietf-curdle-pkix]. After those registrations were done, there were still some unused values that can be used for other security groups.

Object identifiers are primarily used with Abstract Syntax Notation (ASN.1) [ASN.1]. The ASN.1 specifications continue to evolve, but object identifiers can be used with any and all versions of ASN.1.

This document describes the object identifiers that were assigned in that donated range, transfers control of the range to IANA, and establishes IANA allocation policies for any future assignments.

The donated range from DigiCert, Inc. is:

first: { iso (1) identified-organization (3) thawte (101) 100 }
last: { iso (1) identified-organization (3) thawte (101) 127 }

2. IANA Considerations

IANA is asked to create one new registry table.

2.1. "SMI Security for Cryptographic Algorithms" Registry

Within the SMI-numbers registry, add an "SMI Security for Cryptographic Algorithms" table with the three columns:

Decimal	Description	References
0 - 99	Retained by Digicert	[I-D.ietf-curdle-pkix]
100	Reserved for child reg	
110	id-X25519	[I-D.ietf-curdle-pkix]
111	id-X448	[I-D.ietf-curdle-pkix]
112	id-EdDSA25519	[I-D.ietf-curdle-pkix]
113	id-EdDSA448	[I-D.ietf-curdle-pkix]
114	Reserved for id-EdDSA25519-ph	[I-D.ietf-curdle-pkix-03]
115	Reserved for id-EdDSA448-ph	[I-D.ietf-curdle-pkix-03]
128 and up	Retained by Digicert	[I-D.ietf-curdle-pkix]

The column 'Decimal' is required to be a number between 100 and 127 inclusive.

The value of 100 has been reserved so that a new arc below that point can be established in the future. (I.e. starting at 1.3.101.100.1) If the new child registry is established, a name for this value is to be assigned at that point. The experts can, at their discretion, assign an algorithm OID instead.

The registry is to be created using the "Specification Required" policy as defined in [RFC8126].

3. Security Considerations

This document populates an IANA registry, and it raises no new security considerations. The protocols that specify these values include the security considerations associated with their usage.

4. References

4.1. Normative References

[ASN.1] "Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation. ITU-T Recommendation X.680 (2008)", ITU-T X.680, ISO/IEC 8824-1:2008, November 2008.

4.2. Informational References

[I-D.ietf-curdle-pkix] Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519 and X448 for use in the Internet X.509 Public Key Infrastructure", draft-ietf-curdle-pkix-07 (work in progress), November 2017.

[I-D.ietf-curdle-pkix-03] Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519 and X448 for use in the Internet X.509 Public Key Infrastructure", draft-ietf-curdle-pkix-07 (work in progress), November 2016.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/info/rfc7748>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

Acknowledgments

Our thanks go out to DigiCert for donating the range of OIDs covered in this document. At the time of the donation, the root of the range was assigned to Symantec but has sense been transfered DigiCert.

This document uses a lot of text from a similar document by Russ Housley. Copying always makes things easier and less error prone.

Authors' Addresses

Jim Schaad
August Cellars

Email: ietf@augustcellars.com

Rick Andrews
DigiCert, Inc.

Email: rick.andrews@digicert.com