Internet Engineering Task Force (IETF)
Request for Comments: 8411
Category: Informational
ISSN: 2070-1721

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

August 2018

IANA Registration for the Cryptographic Algorithm Object Identifier Range

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 donated range and the identifiers that were assigned from that range, transfers control of that range to IANA, and establishes IANA allocation policies for any future assignments within that range.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8411.

Table of Contents

1. Introduction

When the Curdle Security Working Group was chartered, a range of object identifiers was donated to the working group by DigiCert, Inc. The use of these object identifiers allowed for the Edwards Elliptic 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. The initial registrations from this arc were made while developing [RFC8410]. After those registrations were made, there were still some unused values that could be used by 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 as follows:

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

2. IANA Considerations

IANA has created the "SMI Security for Cryptographic Algorithms" registry within the SMI-numbers registry. The new registry has three columns, as shown below.

Decimal	Description	References
0-99	Retained by DigiCert	RFC 8411
100	Reserved for child reg	RFC 8411
110	id-X25519	[RFC8410]
111	id-X448	[RFC8410]
112	id-EdDSA25519	[RFC8410]
113	id-EdDSA448	[RFC8410]
114	Reserved for id-EdDSA25519-ph	[SAFE-X.509-03]
115	Reserved for id-EdDSA448-ph	[SAFE-X.509-03]
128 and up	Retained by DigiCert	RFC 8411

Table 1: SMI Security for Cryptographic Algorithms

The registration policy is "Specification Required" as defined in [RFC8126].

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.

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

4.2. Informative References

[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>.

[RFC8410] Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure", RFC 8410, DOI 10.17487/RFC8410, August 2018.

[SAFE-X.509-03] Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519 and X448 for use in the Internet X.509 Public Key Infrastructure", Work in Progress, draft-ietf-curdle-pkix-03, November 2016.

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 since been transferred to 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