Using Curve25519 and Curve448 Public Keys in PKIX
draft-josefsson-pkix-newcurves-00

Abstract

   This document specify "named curve" object identifiers for Curve25519
   and Curve448, for use as subject public keys in X.509 PKIX
   Certificates.

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 December 31, 2015.

Copyright Notice

1. Introduction

   In [I-D.irtf-cfrg-curves], Curve25519 and Curve448 are described.
   They are Elliptic Curve Diffie-Hellman (ECDH) functions, designed
   with performance and security in mind.

   This RFC define ASN.1 "named curve" object identifiers for Curve25519
   and Curve448 (aka Goldilocks) public keys, for use in the Internet
   X.509 PKI [RFC5280].

   Rather than defining a new subject public key format for these two
   curves, this document re-use the existing ECDH public-key contained
   (described in section 2.3.5 of [RFC3279]) and introduce two new
   "named curve" OIDs. This approach is the same as for the Brainpool
   curves [RFC5639].

2. Requirements Terminology

   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 [RFC2119].

3. Curve25519 and Curve448 Public Keys

   Certificates conforming to [RFC5280] may convey a public key for any
   public key algorithm. The certificate indicates the algorithm
   through an algorithm identifier. This algorithm identifier is an OID
   and optionally associated parameters. Section 2.3.5 of [RFC3279]
   describe ECDH public keys, specifying the id-ecPublicKey OID. This
   OID has the associated EcpkParameters parameters structure, which
   contains the namedCurve CHOICE. Here we introduce two new OIDs for
   use in the namedCurve field.

       id-Curve25519 OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.11591.7 }
         id-Curve447 OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.11591.8 }

   The OID id-Curve25519 refers to Curve25519. The OID id-Curve448
   refers to Curve448. Both curves are described in
   [I-D.irtf-cfrg-curves].

   The public key value encoded into the ECPoint value is the raw binary
   values described in [I-D.irtf-cfrg-curves].

4. Acknowledgements

   Text and/or inspiration were drawn from [RFC5280], [RFC3279],
   [RFC5480], and [RFC5639].

Several people suggested the utility of specifying OIDs for encoding Curve25519/Curve448 public keys into PKIX certificates, the editor of this document cannot take credit for this idea.

5. IANA Considerations

None.

6. Security Considerations

The security considerations of [RFC3279], [RFC5280], [RFC5480] and [I-D.irtf-cfrg-curves] apply accordingly.

7. References

7.1. Normative References

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
            Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3279]   Bassham, L., Polk, W., and R. Housley, "Algorithms and
            Identifiers for the Internet X.509 Public Key
            Infrastructure Certificate and Certificate Revocation List
            (CRL) Profile", RFC 3279, April 2002.

[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.

[RFC5480]   Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk,
            "Elliptic Curve Cryptography Subject Public Key
            Information", RFC 5480, March 2009.

[I-D.irtf-cfrg-curves]
            Langley, A., Salz, R., and S. Turner, "Elliptic Curves for
            Security", draft-irtf-cfrg-curves-01 (work in progress),
            January 2015.

7.2. Informative References

[RFC5639]   Lochter, M. and J. Merkle, "Elliptic Curve Cryptography
            (ECC) Brainpool Standard Curves and Curve Generation", RFC
            5639, March 2010.

Author's Address

     Simon Josefsson
     SJD AB

     Email: simon@josefsson.org