

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: September 21, 2016

S. Josefsson  
SJD AB  
March 20, 2016

**Using Curve25519 and Curve448 in PKIX  
draft-ietf-curdle-pkix-newcurves-00**

**Abstract**

This document specifies "named curve" object identifiers for the Curve25519 and Curve448 curves, for use in various X.509 PKIX structures.

**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 September 21, 2016.

**Copyright Notice**

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## 1. Introduction

In [\[RFC7748\]](#), the elliptic curves Curve25519 and Curve448 are described. They are designed with performance and security in mind. The curves may be used for Diffie-Hellman and Digital Signature operations.

This RFC define ASN.1 "named curve" object identifiers for Curve25519 and Curve448, 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 ECDSA/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 Named Curve Identifier

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 ECDSA/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 ::= { 1.3.6.1.4.1.11591.15.1 }
id-Curve448      OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.11591.15.2 }
id-Curve25519ph  OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.11591.15.3 }
id-Curve448ph    OBJECT IDENTIFIER ::= { 1.3.6.1.4.1.11591.15.4 }
```

The OID id-Curve25519 refers to Curve25519. The OID id-Curve448 refers to Curve448. Both curves are described in [\[RFC7748\]](#). The OIDs id-Curve25519ph and id-Curve448ph refers to Curve25519 and Curve448 when used with pre-hashing as Ed25519ph and Ed448ph described in [\[I-D.irtf-cfrg-eddsa\]](#).

The public key value encoded into the ECPoint value is the raw binary values described in [\[RFC7748\]](#).



## **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 [\[RFC7748\]](#) 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.
- [RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", [RFC 7748](#), DOI 10.17487/RFC7748, January 2016, <<http://www.rfc-editor.org/info/rfc7748>>.
- [I-D.irtf-cfrg-eddsa] Josefsson, S. and I. Liusvaara, "Edwards-curve Digital Signature Algorithm (EdDSA)", [draft-irtf-cfrg-eddsa-00](#) (work in progress), October 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](mailto:simon@josefsson.org)