PKIX Working Group
INTERNET-DRAFT
Expires December 3, 2001

Daniel R. L. Brown,
Certicom Corp.
June 3, 2002

NIST Recommended EC Domain Parameters For PKIX

<draft-ietf-pkix-ecc-nist-recommended-curves-00.txt>

Status of this Memo

Abstract

This document gives the object identifiers for the elliptic curve domain pararmeters that the National Institute of Standards and Techology recommends in its publication "Digital Signature Standard" (Federal Infomration Processing Standards 186-2). These elliptic curve domain prameters are defined to align PKIX with other ECC implementations and standards. It should be noted that this document is not self-contained. It uses the notations and definitions of [PKIX].

Table of Contents

1. Introduction

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 [RFC 2119].

This document specifies algorithm identifiers and ASN.1 [X.660] encoding formats for digital signatures and subject public keys used in the Internet X.509 Public Key Infrastructure (PKI). This specification supplements [RFC 3279], "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile " Implementations of this specification MUST also conform to RFC 3279.

This specification describes the object identifiers used when identifying elliptic curve domain parameters for elliptic curve public keys. In particular it describes some object identifiers in [ANSI X9.63] "American National Standard for Financial Services X9.63-2001: Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography". These object identifiers are the named curves of [ANSI X9.63] and are convenient way to identify certain elliptic domain parameters. These curves and their object identifiers are also given in [SEC 2] "Recommended Elliptic Curve Domain Parameters".

NIST also recommends these named curves in [FIPS 186-2] "Digital Signature Standard (DSS)".

The fifteen NIST recommended elliptic curve domain parameters have the object identifiers named

```
secp192r1, sect163k1, sect163r2,
secp224r1, sect233k1, sect233r1,
secp256r1, sect283k1, sect283r1,
secp384r1, sect409k1, sect409r1,
secp521r1, sect571k1, sect571r1.
```

The values of these object identifiers are given in [ANSI X9.63], [SEC 2] and Section 2 of this specification. The descriptions of these elliptic curve domain parameters are given in [ANSI X9.63] and [SEC 2].

2. OIDs for NIST Recommnded EC Domain Paramters

The object identifiers for NIST recommended curves extend the object identifiers anxi-x9-62 and ellipticCurve whose values are

```
ansi-x9-62 OBJECT IDENTIFER ::= {
      iso(1) member-body(2) us(840) 10045
}

ellipticCurve OBJECT IDENTIFIER ::= {
  iso(1) identified-organization(3) certicom(132) curve(0)
}
```

The values of the object identifiers for the fifteen NIST recommended curves are

```
secp192r1 OBJECT IDENTIFIER ::= { ansi-x9-62 curves(3) prime(1) 1 }
sect163k1 OBJECT IDENTIFIER ::= { ellipticCurve 1 }
sect163r2 OBJECT IDENTIFIER ::= { ellipticCurve 15 }
secp224r1 OBJECT IDENTIFIER ::= { ellipticCurve 33 }
sect233k1 OBJECT IDENTIFIER ::= { ellipticCurve 26 }
sect233r1 OBJECT IDENTIFIER ::= { ellipticCurve 27 }
secp256r1 OBJECT IDENTIFIER ::= { ansi-x9-62 curves(3) prime(1) 7 }
sect283k1 OBJECT IDENTIFIER ::= { ellipticCurve 16 }
sect283r1 OBJECT IDENTIFIER ::= { ellipticCurve 17 }
secp384r1 OBJECT IDENTIFIER ::= { ellipticCurve 34 }
sect409k1 OBJECT IDENTIFIER ::= { ellipticCurve 36 }
sect409r1 OBJECT IDENTIFIER ::= { ellipticCurve 37 }
secp521r1 OBJECT IDENTIFIER ::= { ellipticCurve 35 }
sect571k1 OBJECT IDENTIFIER ::= { ellipticCurve 38 }
sect571r1 OBJECT IDENTIFIER ::= { ellipticCurve 39 }
```

3. Security Considerations

To be added later.

4. Intellectual Property Rights

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

5. Acknowledgments

To be added later.

6. References

[FIPS 186-2] U.S. Department of Commerce/National Institute of Standards and Technology. Digital Signature Standard (DSS), FIPS PUB 186-2, January 2000. (http://csrc.nist.gov/fips/fips186-2.pdf)

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

[SEC2] Standards for Efficient Cryptography Group. SEC 2 - Recommended Elliptic Curve Domain Parameters. Working Draft Ver. 0.6., 1999. (http://www.secg.org)

[X9.63] American National Standard for Financial Services. ANSI X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography. November 2001.

7. Authors' Addresses

Authors:

Daniel R. L. Brown
Certicom Corp.
dbrown@certicom.com