Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 18, 2015

J. Schmidt
J. Merkle
secunet Security Networks
M. Lochter
BSI

June 16, 2015

# ECC Brainpool Curves for DNSSEC
# draft-schmidt-brainpool-dnssec-03

Abstract

This document specifies the use of ECDSA with ECC Brainpool curves in DNS Security (DNSSEC). It comprises curves of two different sizes.

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 18, 2015.

Table of Contents



## 1. Introduction

In [RFC5639] a new set of elliptic curve groups over finite prime fields for use in cryptographic applications is specified. These groups, denoted as ECC Brainpool curves, were generated in a verifiable pseudo-random way and comply with the security requirements of relevant standards from ISO [ISO1] [ISO2], ANSI [ANSI], NIST [FIPS-186-4], and SecG [SEC2].

[RFC6605] defines the usage of the Elliptic Curve Digital Signature Algorithm (ECDSA) in DNSSEC with two specific NIST curves. This document specifies the use of two additional curves from [RFC5639]. Details on Elliptic Curves and the implementation of ECDSA can be found e.g. in [SEC1], [HMV], [BSI], and [RFC6090].

## 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. ECDSA Parameters

Signer and verifier of an ECDSA signature need to agree on a set of parameters. This document makes use of the Brainpool curves with bit-sizes 256 and 384, specified in Section 3.4 and 3.6 of [RFC5639], and denoted as brainpoolP256r1 and brainpoolP384r1, respectively.

## 4. DNSKEY and RRSIG Resource Records for ECDSA

The records are defined as in [RFC6605]: The ECDSA public key, denoted as "Q" in [FIPS-186-4], is encoded as the bit string "x|y", representing the concatenation of the x and y coordinates of the uncompressed curve point. An ECDSA signature is composed of the

integer values "r" and "s" (see [FIPS-186-4]). Each integer value is encoded as bit string of 32 octets for brainpoolP256r1 and of 48 octets for brainpoolP384r1. The conversion of integers to bit strings is specified in Section C.2 of [FIPS-186-4]. The signature for DNSSEC is encoded as concatenation of the bit strings of "r" and "s", i.e., as "r|s". Hence, the ECDSA signature has a fixed length of 64 octets for brainpoolP256r1 and 96 octets for brainpoolP384r1.

The IANA Considerations section defines the algorithm numbers used for DNSKEY and RRSIG resource records.

> Algorithm number TBD1 for using ECDSA with brainpoolP256r1 and SHA-256 for DNSKEY and RRSIG Resource Records.
>
> Algorithm number TBD2 for using ECDSA with brainpoolP384r1 and SHA-384 for DNSKEY and RRSIG Resource Records.

The use of these algorithms is OPTIONAL: an implementer can choose to support any subset.

## 5. Support for NSEC3 Denial of Existence

The statement of [RFC6605] applies.

## 6. IANA Considerations

IANA is requested to assign numbers for ECDSA with ECC Brainpool curves listed in Section 3 to "Domain Name System Security (DNSSEC) Algorithm Numbers". In the following the two new entries are listed.

| | |
|---|---|
| Number | TBD1 |
| Description | ECDSA Curve brainpoolP256r1 with SHA-256 |
| Mnemonic | ECDSAbrainpoolP256r1SHA256 |
| Zone Signing | Y |
| Trans. Sec | * |
| Reference | This document |

| | |
|---|---|
| Number | TBD2 |
| Description | ECDSA Curve brainpoolP384r1 with SHA-384 |
| Mnemonic | ECDSAbrainpoolP384r1SHA384 |
| Zone Signing | Y |
| Trans. Sec | * |
| Reference | This document |

> * There has been no determination of standardization of the use of this algorithm with Transaction Security.

## 7. Security Considerations

The security considerations of [RFC5639], [RFC6605], and [RFC4509] apply accordingly.

## 8. References

### 8.1. Normative References

[FIPS-186-4] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB 186-4, July 2013.

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

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, May 2006.

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

[RFC6605] Hoffman, P. and W. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, April 2012.

### 8.2. Informative References

[ANSI] American National Standards Institute, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62, 2005.

[BSI] Bundesamt fuer Sicherheit in der Informationstechnik, "Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations", July 2011.

[HMV] Hankerson, D., Menezes, A., and S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer Verlag, 2004.

[ISO1] International Organization for Standardization, "Information Technology - Security Techniques - Digital Signatures with Appendix - Part 3: Discrete Logarithm Based Mechanisms", ISO/IEC 14888-3, 2006.

[ISO2] International Organization for Standardization, "Information Technology - Security Techniques - Cryptographic Techniques Based on Elliptic Curves - Part 2: Digital signatures", ISO/IEC 15946-2, 2002.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, February 2011.

[SEC1] Certicom Research, "Elliptic Curve Cryptography, Version 2.0", Standards for Efficient Cryptography (SEC) 1, May 2009.

[SEC2] Certicom Research, "Recommended Elliptic Curve Domain Parameters, Version 2.0", Standards for Efficient Cryptography (SEC) 2, January 2010.

## Authors' Addresses

Joern-Marc Schmidt
secunet Security Networks
Mergenthaler Allee 77
65760 Eschborn
Germany

Phone: +49 201 5454 3694
EMail: joern-marc.schmidt@secunet.com

Johannes Merkle
secunet Security Networks
Mergenthaler Allee 77
65760 Eschborn
Germany

Phone: +49 201 5454 3091
EMail: johannes.merkle@secunet.com

Manfred Lochter
BSI
Postfach 200363
53133 Bonn
Germany

Phone: +49 228 9582 5643
EMail: manfred.lochter@bsi.bund.de