Network Working Group P. Hoffman
Internet-Draft VPN Consortium
Intended status: Informational W. Wijngaards
Expires: June 4, 2011 NLnet Labs
December 1, 2010

Elliptic Curve DSA for DNSSEC
draft-hoffman-dnssec-ecdsa-04

Abstract

This document describes how to specify Elliptic Curve DSA keys and signatures in DNSSEC. It lists curves of different sizes, and uses the SHA-2 family of hashes for signatures.

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 June 4, 2011.

Copyright Notice

Copyright (c) 2010 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.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

1. Introduction

DNSSEC, which is broadly defined in RFCs 4033, 4034, and 4035 ([RFC4033], [RFC4034], and [RFC4035]), uses cryptographic keys and digital signatures to provide authentication of DNS data. Currently, the most popular signature algorithm is RSA with SHA-1, using keys 1024 or 2048 bits long.

This document defines the DNSKEY and RRSIG resource records (RRs) of two new signing algorithms: ECDSA with curve P-256 and SHA-256, and ECDSA with curve P-384 and SHA-384. This document also defines the DS RR for the SHA-384 one-way hash algorithm; the associated DS RR for SHA-256 is already defined in RFC 4509 [RFC4509].

Current estimates are that ECDSA with curve P-256 has an approximate equivalent strength to RSA with 3072-bit keys. Using ECDSA with curve P-256 in DNSSEC has some advantages and disadvantages relative to using RSA with SHA-256 and with 3072-bit keys. ECDSA keys are much shorter than RSA keys; at this size, the difference is 256 versus 3072 bits. Similarly, ECDSA signatures are much shorter than RSA signatures. This is relevant because DNSSEC stores and transmits both keys and signatures.

In the two signing algorithms defined in this document, the size of the key for the elliptic curve is matched with the size of the output of the hash algorithm. This design is based on the widespread belief that the equivalent strength of P-256 and P-384 is half the length of the key, and also that the equivalent strength of SHA-256 and SHA-384 is half the length of the key. Using matched strengths prevents an attacker from chosing the weaker half of a signature algorithm. For example, in a signature that uses RSA with 2048-bit keys and SHA-256, the signing portion is significantly weaker than the hash portion, whereas the two algorithms here are balanced.

Signing with ECDSA is significantly faster than with RSA (over 20

times in some implementations). However, validating RSA signatures is significantly faster than validating ECDSA signatures (about 5 times faster in some implementations).

Some of the material in this document is copied liberally from RFC 5430 [RFC5430].

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 [RFC2119].

2. SHA-384 DS Records

SHA-384 is defined in FIPS 180-3 [FIPS-180-3] and RFC 4634 [RFC4634], and is similar to SHA-256 in many ways. The implementation of SHA-384 in DNSSEC follows the implementation of SHA-256 as specified in RFC 4509 except that the underlying algorithm is SHA-384, the digest value is 48 bytes long, and the digest type code is {TBA-1}.

3. ECDSA Parameters

Verifying ECDSA signatures requires agreement between the signer and the verifier of the parameters used. FIPS 186-3 [FIPS-186-3] lists some NIST-recommended elliptic curves. (Other documents give more detail on ECDSA than is given in FIPS 186-3.) These are the same curves as listed in RFC 5114 [RFC5114]. The curves used in this document are:

FIPS 186-3	RFC 5114
P-256 (Section D.1.2.3)	256-bit Random ECP Group (Section 2.6)
P-384 (Section D.1.2.4)	384-bit Random ECP Group (Section 2.7)

4. DNSKEY and RRSIG Resource Records for ECDSA

ECDSA public keys consist of a single value, called "Q" in FIPS 186-3. In DNSSEC keys, Q is a simple bit string that represents the uncompressed form of a curve point, "x | y".

The ECDSA signature is the combination of two non-negative integers, called "r" and "s" in FIPS 186-3. The two integers, each of which is formatted as a simple octet string, are combined into a single longer octet string for DNSSEC as the concatenation "r | s".

The algorithm numbers associated with the DNSKEY and RRSIG resource

records are fully defined in the IANA Considerations section. They are:

- o DNSKEY and RRSIG RRs signifying ECDSA with the P-256 curve and SHA-256 use the algorithm number {TBA-2}.
- o DNSKEY and RRSIG RRs signifying ECDSA with the P-384 curve and SHA-384 use the algorithm number {TBA-3}.

Conformant implementations MUST support signing and/or validation of signatures with both ECDSA with the P-256 curve and SHA-256, and with ECDSA with the P-384 curve and SHA-384.

5. Support for NSEC3 Denial of Existence

RFC 5155 [RFC5155] defines new algorithm identifiers for existing signing algorithms, to indicate that zones signed with these algorithm identifiers can use NSEC3 as well as NSEC records to provide denial of existence. That mechanism was chosen to protect implementations predating RFC 5155 from encountering resource records they could not know about. This document does not define such algorithm aliases.

A DNSSEC validator that implements the signing algorithms defined in this document MUST be able to validate negative answers in the form of both NSEC and NSEC3 with hash algorithm 1, as defined in RFC 5155. An authoritative server that does not implement NSEC3 MAY still serve zones that use the signing algorithms defined in this document with NSEC denial of existence.

6. Examples

The following are some examples of ECDSA keys and signatures in DNS format.

[[IMPORTANT NOTE: This section is to be used for testing only. This document has not been approved as an RFC, so the algorithm codes MUST NOT be used on the Internet, only in test environments. The examples use {TBA-1}: 4, {TBA-2}: 13, {TBA-3}: 14.]]

6.1. P-256 Example

```
   Private-key-format: v1.2
   Algorithm: 13 (ECDSAP256SHA256)
   PrivateKey: GU6SnQ/Ou+xC5RumuIUIuJZteXT2z0O/ok1s38Et6mQ=

   example.net. 3600 IN DNSKEY 257 3 13 (
           GojIhhXUN/u4v54ZQqGSnyhWJwaubCvTmeexv7bR6edb
           krSqQpF64cYbcB7wNcP+e+MAnLr+Wi9xMWyQLc8NAA== )

   example.net. 3600 IN DS 55648 13 2 (
           b4c8c1fe2e7477127b27115656ad6256f424625bf5c1
           e2770ce6d6e37df61d17 )

   www.example.net. 3600 IN A 192.0.2.1
   www.example.net. 3600 IN RRSIG A 13 3 3600 (
           20100909100439 20100812100439 55648 example.net.
           qx6wLYqmh+l9oCKTN6qIc+bw6ya+KJ8oMz0YP107epXA
           yGmt+3SNruPFKG7tZoLBLlUzGGus7ZwmwWep666VCw== )
```

6.2. P-384 Example

```
   Private-key-format: v1.2
   Algorithm: 14 (ECDSAP384SHA384)
   PrivateKey: WURgWHCcYIYUPWgeLmiPY2DJJk02vgrmTfitxgqcL4vw
   W7BOrbawVmVe0d9V94SR

   example.net. 3600 IN DNSKEY 257 3 14 (
           xKYaNhWdGOfJ+nPrL8/arkwf2EY3MDJ+SErKivBVSum1
           w/egsXvSADtNJhyem5RCOpgQ6K8X1DRSEkrbYQ+OB+v8
           /uX45NBwY8rp65F6Glur8I/mlVNgF6W/qTI37m40 )

   example.net. 3600 IN DS 10771 14 4 (
           72d7b62976ce06438e9c0bf319013cf801f09ecc84b8
           d7e9495f27e305c6a9b0563a9b5f4d288405c3008a94
           6df983d6 )

   www.example.net. 3600 IN A 192.0.2.1
   www.example.net. 3600 IN RRSIG A 14 3 3600 (
           20100909102025 20100812102025 10771 example.net.
           /L5hDKIvGDyI1fcARX3z65qrmPsVz73QD1Mr5CEqOiLP
           95hxQouuroGCeZOvzFaxsT8Glr74hbavRKayJNuydCuz
           WTSSPdz7wnqXL5bdcJzusdnI0RSMROxxwGipWcJm )
```

7. IANA Considerations

This document updates the IANA registry for digest types in DS records, currently called "Delegation Signer Resource Record, Digest Algorithms". The following entry is added:

Value	{TBA-1}
Digest Type	SHA-384
Status	OPTIONAL

This document updates the IANA registry "Domain Name System Security (DNSSEC) Algorithm Numbers". The following two entries are added to the registry:

Number	{TBA-2}
Description	ECDSA Curve P-256 with SHA-256
Mnemonic	ECDSAP256SHA256
Zone Signing	Y
Trans. Sec.	*
Reference	This document

Number	{TBA-3}
Description	ECDSA Curve P-384 with SHA-384
Mnemonic	ECDSAP384SHA384
Zone Signing	Y
Trans. Sec.	*
Reference	This document

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

8. Security Considerations

The cryptographic strength of ECDSA with curve P-256 or P-384 is generally considered to be equivalent to half the size of the key, or 128 bits and 192 bits, respectively. Such an assessment could, of course, change in the future if new attacks that work better than the ones known today are found.

The security considerations listed in RFC 4509 apply here as well.

9. References

9.1. Normative References

[FIPS-180-3]
National Institute of Standards and Technology, U.S. Department of Commerce, "Secure Hash Standard (SHS)", FIPS 180-3, October 2008.

[FIPS-186-3]
National Institute of Standards and Technology, U.S. Department of Commerce, "Digital Signature Standard", FIPS 186-3, June 2009.

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

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

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

[RFC5114] Lepinski, M. and S. Kent, "Additional Diffie-Hellman Groups for Use with IETF Standards", RFC 5114, January 2008.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.

9.2. Informative References

[RFC4634] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, July 2006.

[RFC5430] Salter, M., Rescorla, E., and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 5430, March 2009.

Appendix A. Change History

This entire section should be removed before publication as an RFC.

A.1. Changes betweeen draft-hoffman-dnssec-ecdsa-00 and -01

Numerous editorial fixes from Alfred Hoenes.

In the IANA Considerations, used the same wording about TSIG as is used in draft-ietf-dnsext-dnssec-rsasha256-14: "There has been no determination of standardization of the use of this algorithm with Transaction Security."

A.2. Changes betweeen draft-hoffman-dnssec-ecdsa-01 and -02

None; version bump.

A.3. Changes betweeen draft-hoffman-dnssec-ecdsa-02 and -03

Added Wouter Wijngaards as co-author.

Removed ECDSAP224SHA256 to simplify.

The DNSKEY is defined as being stored as "x | y".

Added examples.

A.4. Changes betweeen draft-hoffman-dnssec-ecdsa-03 and -04

In section 4, made "r", "s", and "r | s" octet strings instead of bit strings.

Added pointer to RFC 4509 in the Security Considerations.

Added paragraph describing why we used balanced strengths in the defined algorithms.

Authors' Addresses

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org

Wouter Wijngaards
NLnet Labs

Email: wouter@nlnetlabs.nl