Internet Engineering Task Force (IETF)
Request for Comments: 6605
Category: Standards Track
ISSN: 2070-1721

P. Hoffman
VPN Consortium
W.C.A. Wijngaards
NLnet Labs

April 2012

Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC

Abstract

This document describes how to specify Elliptic Curve Digital Signature Algorithm (DSA) keys and signatures in DNS Security (DNSSEC). It lists curves of different sizes and uses the SHA-2 family of hashes for signatures.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6605.

Copyright Notice

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 that are 1024 or 2048 bits long.

This document defines the DNSKEY and RRSIG resource records (RRs) of two new signing algorithms: ECDSA (Elliptic Curve DSA) with curve P-256 and SHA-256, and ECDSA with curve P-384 and SHA-384. (A description of ECDSA can be found in [FIPS-186-3].) 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]. [RFC6090] provides a good introduction to implementing ECDSA.

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 choosing 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 6460 [RFC6460].

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 6234 [RFC6234], 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 4.

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 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". (Conversion of the integers to bit strings is described in Section C.2 of FIPS 186-3.) For P-256, each integer MUST be encoded as 32 octets; for P-384, each integer MUST be encoded as 48 octets.

The algorithm numbers associated with the DNSKEY and RRSIG resource records are fully defined in the IANA Considerations section. They are:

- DNSKEY and RRSIG RRs signifying ECDSA with the P-256 curve and SHA-256 use the algorithm number 13.

- DNSKEY and RRSIG RRs signifying ECDSA with the P-384 curve and SHA-384 use the algorithm number 14.

Conformant implementations that create records to be put into the DNS MUST implement signing and verification for both of the above algorithms. Conformant DNSSEC verifiers MUST implement verification for both of the above algorithms.

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.

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 (DS) Resource Record (RR) Type Digest Algorithms". The following entry has been added:

Value	4
Digest Type	SHA-384
Status	OPTIONAL

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

Number	13
Description	ECDSA Curve P-256 with SHA-256
Mnemonic	ECDSAP256SHA256
Zone Signing	Y
Trans. Sec.	*
Reference	This document

Number	14
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 work factor 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

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

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, May 2011.

[RFC6460] Salter, M. and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 6460, January 2012.

Authors' Addresses

Paul Hoffman
VPN Consortium

EMail: paul.hoffman@vpnc.org

Wouter C.A. Wijngaards
NLnet Labs

EMail: wouter@nlnetlabs.nl