DSA with SHA-2 for DNSSEC

draft-hoffman-dnssec-dsa-sha2-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. 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.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 7, 2010.

Copyright Notice

Copyright (c) 2009 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
This document describes how to specify DSA keys and signatures based on SHA-256 with a specific set of parameters in DNSSEC. The keys used are 2048 bits, and have an equivalent security level of 112 bits.

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. The RSA with SHA-256 signature algorithm (as specified in [RSASHA256]) with keys of 1024 to 2048 bits is expected to become popular in the coming years.

RFC 2536 [RFC2536] describes the KEY and SIG resource records (RRs) for the DSA with SHA-1 signature algorithm. At the time RFC 2536 was written, SHA-1 was the only hash algorithm that was defined for use with DSA, and the only key size allowed was 1024 bits. FIPS 186-3 ([FIPS-186-3]) extends the original DSA definition to permit larger keys. This document neither updates nor replaces RFC 2536.

Using DSA with SHA-256 in DNSSEC has some advantages and disadvantages relative to using RSA with SHA-256 when using 2048-bit keys. DSA signatures are much shorter than RSA signatures; at this size, the difference is 512 bits versus 2048 bits. On typical platforms using 2048-bit keys, signing DSA is about three times faster than for RSA, but verifying RSA signatures is more than ten times faster than for DSA.

This document specifies the DNSKEY and RRSIG RRs for DSA when used with the SHA-256 hash algorithm for a specific set of DSA parameters from RFC 5114 [RFC5114].

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. DSA Parameters

In order for a DSA signature to be validated, the validator needs to know the DSA parameters that were used. The three parameters are called "p", "q", and "g" in FIPS 186-3. FIPS 186-3 calls the private key "x" and the public key "y"; the per-signature secret value is called "k".

In some cryptographic protocols, the signer picks their own parameters and transmits them with the signature. However, because of their size, this is often wasteful of bandwidth and storage. Other cryptographic protocols pick well-known parameters that are used by everyone, and the only thing that is passed is an indicator of which parameter set is used.

Because DNS messages should be kept short, this document chooses the latter method. The parameters are chosen following the methods described in FIPS 186-3. The size of the parameters is based on the desired strength of the signatures. This document uses DSA with SHA-256 and a 2048-bit y, the public key. Thus, p is 2048 bits, q is 256 bits, and g is 2048 bits long.

The values used in this document are from RFC 5114, section 2.3. In hexadecimal, they are:
3. DNSKEY and RRSIG Resource Records for DSA with SHA-256

The DSA signature is the combination of two non-negative integers, called "r" and "s" in FIPS 186-3. Because q was chosen to be the same size as the output of SHA-256 (256 bits), r and s are each 256 bits. The two integers, each of which is formatted as a simple bit string, are combined into a single longer bit string for DNSSEC as the concatenation "r | s".

The algorithm number associated with the DNSKEY and RRSIG resource records for DSA with SHA-256 and the parameters in this document is (TBA); it is fully defined in the IANA Considerations section. The associated DS RR for SHA-256 is already defined in RFC 4509 [RFC4509].

4. 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 algorithm 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 algorithm defined in this document with NSEC denial of existence.

5. Examples

[[ To be filled in later. ]]

6. IANA Considerations

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

Number         {TBA}
Description     DSA with SHA-256 using parameters from RFC 5114, section 2.3
Mnemonic        DSA2048SHA256
Zone Signing    Y
Trans. Sec.     **** Unknown; will fill in later ****
Reference       This document

7. Security Considerations

The cryptographic strength of DSA is generally considered to be equivalent to RSA when the DSA public key and the RSA public keys are the same size. Such an assessment could, of course, change in the future if new attacks that work better with one or the other algorithms are found.

There are currently no known attacks on the specific set of DSA parameters chosen for this document. Such an assessment could, of course, change in the future.

8. References
8.1. Normative References


8.2. Informative References


Author’s Address

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org