                    DNS Security Extensions (DNSSEC)
                        draft-hoffman-dnssec-00

Abstract

   This document describes the DNS security extensions (commonly called
   "DNSSEC") that are specified RFCs 4033, 4034, 4035, and a handful of
   others. The purpose is to introduce all of the RFCs in one place so
   that the reader can understand the many aspects of DNSSEC. This
   document does not update any of those RFCs.

   This document is currently maintained at
   https://github.com/paulehoffman/draft-hoffman-dnssec. Issues and
   pull requests are welcomed. If the document is later adopted by a
   working group, a new repository will likely be created.

Table of Contents

1. Introduction

   The core specification for what we know as DNSSEC (the combination of
   [RFC4033], [RFC4034], and [RFC4035]) describes a set of protocols
   that provides origin authentication to data in the DNS. [RFC6840]
   updates and extends those core RFCs, but does not fundamentally
   change the way that DNSSEC works.

   This document lists many (but not all) of the RFCs that should be
   considered by someone creating an implementation of, or someone
   deploying, modern DNSSEC. It uses terminology from those documents
   without defining that terminology. It also points to the relevant
   IANA registries that relate to DNSSEC. It does not, however, point
   to standards that rely on zones needing to be signed by DNSSEC.

1.1. DNSSEC as a Best Current Practice

   The DNSSEC set of protocols is widely considered the best current
   practice for adding origin authentication of data in the DNS. To
   date, no standards-track RFCs offer any other method for such origin
   authentication of data in the DNS.

   Some observers note that, more than 15 years after the DNSSEC
   specification was published, it is still not widely deployed. Recent
   estimates are that fewer than 10% of the domain names used for web
   sites are signed, and only around a third of queries to recursive
   resolvers are validated. However, this low level of implementation
   does not affect whether DNSSEC is a best current practice; it just
   indicates that the value of deploying DNSSEC is often considered
   lower than the cost.

2. DNSSEC Core Documents

   What we today call "DNSSEC" is formally version 3 of the DNSSEC
   specification. However, earlier versions of DNSSEC were thinly
   deployed and significantly less visible than the current DNSSEC
   specification. Throughout this document, "DNSSEC" means the version
   of the protocol initially defined in [RFC4033], [RFC4034], and
   [RFC4035].

   The three initial core documents generally cover different topics:

   * [RFC4033] is an overview of DNSSEC, including how it might change
      the resolution of DNS queries.

   * [RFC4034] specifies the DNS resource records used in DNSSEC. It
      obsoletes many RFCs for earlier versions of DNSSEC.

   * [RFC4035] covers the modifications to the DNS protocol incurred by
      DNSSEC. These include signing zones, serving signed zones,
      resolving in light of DNSSEC, and authenticating DNSSEC-signed
      data.

   At the time this set of core documents was published, someone could
   create a DNSSEC implementation of signing software, of an DNSSEC-
   aware authoritative server, and/or a DNSSEC-aware recursive resolver
   from the three core documents plus a few older RFCs specifying the
   cryptography used. Those two older documents are:

* [RFC2536] defines how to use the DSA signature algorithm (although refers to other documents for the details). DSA was thinly implemented and can safely be ignored by DNSSEC implementations

* [RFC3110] defines how to use the RSA signature algorithm (although refers to other documents for the details). RSA is still the most popular signing algorithm for DNSSEC.

2.1. Addition to the DNSSEC Core

As with any major protocol, developers and operators discovered issues with the original core documents over the years. [RFC6840] is an omnibus update to the original core documents and thus itself has become a core document. In addition to covering new requirements from new DNSSEC RFCs, it describes many important security and interoperability issues that arose during the deployment of the initial specifications, particularly after the DNS root was signed in 2010. It also lists some errors in the examples of the core specifications.

[RFC6840] brings a few additions into the core of DNSSEC. It makes NSEC3 [RFC5155] as much a part of DNSSEC as NSEC is. It also makes the SHA-2 hash function defined in [RFC4509] and [RFC5702] part of the core as well. # Cryptographic Algorithms and DNSSEC

Cryptography improves over time, and new algorithms get adopted by various Internet protocols. Two new signing algorithms have been adopted by the DNSSEC community: ECDSA [RFC6605] and EdDSA [RFC8080]. The GOST signing algorithm [RFC5933] was also adopted, but has seen very limited use, likely because it is a national algorithm specific to a very small number of countries.

Implementation developers who want to know which algorithms to implement in DNSSEC software should refer to [RFC8624]. Note that this specification is only about what algorithms should and should not be included in implementations: it is not advice for which algorithms that zone operators should and should not sign with, nor

which algorithms recursive resolver operators should or should not validate.

3. Extensions to DNSSEC

The DNSSEC community has extended the DNSSEC core and the cryptographic algorithms both in terms of describing good operational practices and in new protocols. Some of the RFCs that describe these extensions include:

*   [RFC5011] explains how recursive resolvers and the DNS root can work together to automate the rollover of the root's key signing key (KSK).

*   [RFC6781] is a compendium of operational practices that may not be obvious from reading just the core specifications.

*   [RFC7344] describes using the CDS and CDNSKEY resource records to help automate the creation of DS records in the parents of signed zones.

*   [RFC8078] extends [RFC7344] by showing how to do initial setup of trusted relationships between signed parent and child zones.

*   [RFC8198] describes how a validating resolver can emit fewer queries in signed zones that use NSEC for negative caching.

*   [RFC9077] updates [RFC8198] with respect to the time-to-live (TTL) fields in signed records.

4. IANA Considerations

IANA already has two registries that relate to DNSSEC: DNSSEC algorithm numbers (https://www.iana.org/assignments/dns-sec-alg-numbers) and DNSSEC NSEC3 parameters (https://www.iana.org/assignments/dnssec-nsec3-parameters). The rules for the DNSSEC algorithm registry were set in the core RFCs and updated by [RFC6014] and [RFC9157].

This document does not create any new IANA considerations.

5. Security Considerations

All of the security considerations from all of the RFCs referenced in this document apply here.

6. References

6.1. Normative References

[RFC3110] Eastlake 3rd, D., "RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS)", RFC 3110, DOI 10.17487/RFC3110, May 2001, <https://www.rfc-editor.org/info/rfc3110>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC4509] Hardaker, W., "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)", RFC 4509, DOI 10.17487/RFC4509, May 2006, <https://www.rfc-editor.org/info/rfc4509>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

   [RFC5702] Jansen, J., "Use of SHA-2 Algorithms with RSA in DNSKEY
              and RRSIG Resource Records for DNSSEC", RFC 5702,
              DOI 10.17487/RFC5702, October 2009,
              <https://www.rfc-editor.org/info/rfc5702>.

   [RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and
              Implementation Notes for DNS Security (DNSSEC)", RFC 6840,
              DOI 10.17487/RFC6840, February 2013,
              <https://www.rfc-editor.org/info/rfc6840>.

6.2. Informative References

   [RFC2536] Eastlake 3rd, D., "DSA KEYs and SIGs in the Domain Name
              System (DNS)", RFC 2536, DOI 10.17487/RFC2536, March 1999,
              <https://www.rfc-editor.org/info/rfc2536>.

   [RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC)
              Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011,
              September 2007, <https://www.rfc-editor.org/info/rfc5011>.

   [RFC5933] Dolmatov, V., Ed., Chuprina, A., and I. Ustinov, "Use of
              GOST Signature Algorithms in DNSKEY and RRSIG Resource
              Records for DNSSEC", RFC 5933, DOI 10.17487/RFC5933, July
              2010, <https://www.rfc-editor.org/info/rfc5933>.

   [RFC6014] Hoffman, P., "Cryptographic Algorithm Identifier
              Allocation for DNSSEC", RFC 6014, DOI 10.17487/RFC6014,
              November 2010, <https://www.rfc-editor.org/info/rfc6014>.

   [RFC6605] Hoffman, P. and W.C.A. Wijngaards, "Elliptic Curve Digital
              Signature Algorithm (DSA) for DNSSEC", RFC 6605,
              DOI 10.17487/RFC6605, April 2012,
              <https://www.rfc-editor.org/info/rfc6605>.

   [RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC
              Operational Practices, Version 2", RFC 6781,
              DOI 10.17487/RFC6781, December 2012,
              <https://www.rfc-editor.org/info/rfc6781>.

   [RFC7344] Kumari, W., Gudmundsson, O., and G. Barwood, "Automating
              DNSSEC Delegation Trust Maintenance", RFC 7344,
              DOI 10.17487/RFC7344, September 2014,

                 <https://www.rfc-editor.org/info/rfc7344>.

   [RFC8078]   Gudmundsson, O. and P. Wouters, "Managing DS Records from
               the Parent via CDS/CDNSKEY", RFC 8078,
               DOI 10.17487/RFC8078, March 2017,
               <https://www.rfc-editor.org/info/rfc8078>.

   [RFC8080]   Sury, O. and R. Edmonds, "Edwards-Curve Digital Security
               Algorithm (EdDSA) for DNSSEC", RFC 8080,
               DOI 10.17487/RFC8080, February 2017,
               <https://www.rfc-editor.org/info/rfc8080>.

   [RFC8198]   Fujiwara, K., Kato, A., and W. Kumari, "Aggressive Use of
               DNSSEC-Validated Cache", RFC 8198, DOI 10.17487/RFC8198,
               July 2017, <https://www.rfc-editor.org/info/rfc8198>.

   [RFC8624]   Wouters, P. and O. Sury, "Algorithm Implementation
               Requirements and Usage Guidance for DNSSEC", RFC 8624,
               DOI 10.17487/RFC8624, June 2019,
               <https://www.rfc-editor.org/info/rfc8624>.

   [RFC9077]   van Dijk, P., "NSEC and NSEC3: TTLs and Aggressive Use",
               RFC 9077, DOI 10.17487/RFC9077, July 2021,
               <https://www.rfc-editor.org/info/rfc9077>.

   [RFC9157]   Hoffman, P., "Revised IANA Considerations for DNSSEC",
               RFC 9157, DOI 10.17487/RFC9157, December 2021,
               <https://www.rfc-editor.org/info/rfc9157>.

Author's Address

   Paul Hoffman
   ICANN
   Email: paul.hoffman@icann.org