Workgroup: Network Working Group
Internet-Draft: draft-ietf-dnsop-dnssec-bcp-01
Published: 14 April 2022
Intended Status: Best Current Practice
Expires: 16 October 2022
Authors: P. Hoffman
ICANN

DNS Security Extensions (DNSSEC)

Abstract

This document describes the DNS security extensions (commonly called "DNSSEC") that are specified RFCs 4033, 4034, 4035, and a handful of others. One 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. Another purpose is to move DNSSEC to Best Current Practice status.

This document is currently maintained at https://github.com/paulehoffman/draft-hoffman-dnssec. Issues and pull requests are welcomed.

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 https://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 16 October 2022.

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 provide 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. Nonetheless, the significant deployment of DNSSEC within some top-level domains (TLDs), and the near-universal deployment of DNSSEC in the TLDs, demonstrate that DNSSEC is suitable for implementation by both ordinary and highly sophisticated domain owners.

1.2. Implementing DNSSEC

Developers of validating resolvers and authoritative servers, as well as operators of operators of validating resolvers and authoritative servers, need to know the parts of the DNSSEC protocol that would affect them. They should read the DNSSEC core documents, and probably at least be familiar with the extensions. Developers will probably need to be very familiar with the algorithm documents as well.

As a side note, some of the DNSSEC-related RFCs have significant errata, so reading the RFCs should also include looking for the related errata.

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.

3. Additional 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.

4. 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.

5. Additional Documents of Interest

The documents listed above constitute the core of DNSSEC, the additional cryptographic algorithms, and the major extensions to DNSSEC. This section lists some additional documents that someone interested in implementing or operating DNSSEC might find of value.

* [RFC4470] "describes how to construct DNSSEC NSEC resource records that cover a smaller range of names than called for by [RFC4034]".

* [RFC6975] "specifies a way for validating end-system resolvers to signal to a server which digital signature and hash algorithms they support".

* [RFC7129] "provides additional background commentary and some context for the NSEC and NSEC3 mechanisms used by DNSSEC to provide authenticated denial-of-existence responses".

* [RFC7583] "describes the issues surrounding the timing of events in the rolling of a key in a DNSSEC-secured zone".

* [RFC7646] "defines Negative Trust Anchors (NTAs), which can be used to mitigate DNSSEC validation failures by disabling DNSSEC validation at specified domains".

* [RFC7958] "describes the format and publication mechanisms IANA has used to distribute the DNSSEC trust anchors".

* [RFC8027] "describes problems that a Validating DNS resolver, stub-resolver, or application might run into within a non-compliant infrastructure".

* [RFC8145] "specifies two different ways for validating resolvers to signal to a server which keys are referenced in their chain of trust".

* [RFC8499] is a list of terminology used when talking about the DNS; sections 10 and 11 cover DNSSEC.

* [RFC8509] "specifies a mechanism that will allow an end user and third parties to determine the trusted key state for the root key of the resolvers that handle that user's DNS queries".

* [RFC8901] "presents deployment models that accommodate this scenario [when each DNS provider independently signs zone data with their own keys] and describes these key-management requirements".

There will certainly be other RFCs related to DNSSEC that are published after this one.

6. IANA Considerations

IANA already has three registries that relate to DNSSEC:

* DNSSEC algorithm numbers (https://www.iana.org/assignments/dns-sec-alg-numbers)

* DNSSEC NSEC3 parameters (https://www.iana.org/assignments/dnssec-nsec3-parameters)

* DNSSEC DS RRtype digest algorithms (https://www.iana.org/assignments/ds-rr-types)

The rules for the DNSSEC algorithm registry were set in the core RFCs and updated by [RFC6014], [RFC6725], and [RFC9157].

This document does not update or create any registries.

7. Security Considerations

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

8. References

8.1. 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>.

8.2. 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>.

[RFC4470] Weiler, S. and J. Ihren, "Minimally Covering NSEC Records and DNSSEC On-line Signing", RFC 4470, DOI 10.17487/RFC4470, April 2006, <https://www.rfc-editor.org/info/rfc4470>.

[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>.

[RFC6725] Rose, S., "DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates", RFC 6725, DOI 10.17487/RFC6725, August 2012, <https://www.rfc-editor.org/info/rfc6725>.

[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>.

[RFC6975] Crocker, S. and S. Rose, "Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC)", RFC 6975, DOI 10.17487/RFC6975, July 2013, <https://www.rfc-editor.org/info/rfc6975>.

[RFC7129] Gieben, R. and W. Mekking, "Authenticated Denial of Existence in the DNS", RFC 7129, DOI 10.17487/RFC7129, February 2014, <https://www.rfc-editor.org/info/rfc7129>.

[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>.

[RFC7583] Morris, S., Ihren, J., Dickinson, J., and W. Mekking, "DNSSEC Key Rollover Timing Considerations", RFC 7583,

DOI 10.17487/RFC7583, October 2015, <https://www.rfc-editor.org/info/rfc7583>.

[RFC7646] Ebersman, P., Kumari, W., Griffiths, C., Livingood, J., and R. Weber, "Definition and Use of DNSSEC Negative Trust Anchors", RFC 7646, DOI 10.17487/RFC7646, September 2015, <https://www.rfc-editor.org/info/rfc7646>.

[RFC7958] Abley, J., Schlyter, J., Bailey, G., and P. Hoffman, "DNSSEC Trust Anchor Publication for the Root Zone", RFC 7958, DOI 10.17487/RFC7958, August 2016, <https://www.rfc-editor.org/info/rfc7958>.

[RFC8027] Hardaker, W., Gudmundsson, O., and S. Krishnaswamy, "DNSSEC Roadblock Avoidance", BCP 207, RFC 8027, DOI 10.17487/RFC8027, November 2016, <https://www.rfc-editor.org/info/rfc8027>.

[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>.

[RFC8145] Wessels, D., Kumari, W., and P. Hoffman, "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)", RFC 8145, DOI 10.17487/RFC8145, April 2017, <https://www.rfc-editor.org/info/rfc8145>.

[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>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC8509] Huston, G., Damas, J., and W. Kumari, "A Root Key Trust Anchor Sentinel for DNSSEC", RFC 8509, DOI 10.17487/RFC8509, December 2018, <https://www.rfc-editor.org/info/rfc8509>.

[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>.

[RFC8901] Huque, S., Aras, P., Dickinson, J., Vcelak, J., and D. Blacka, "Multi-Signer DNSSEC Models", RFC 8901, DOI 10.17487/RFC8901, September 2020, <https://www.rfc-editor.org/info/rfc8901>.

[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>.

Appendix A. Acknowledgements

The DNS world owes a depth of gratitude to the authors and other contributors to the core DNSSEC documents, and to the notable DNSSEC extensions.

In addition, the following people made significant contributions to early versions of this document: Ben Schwartz and Duane Wessels.

Author's Address

Paul Hoffman
ICANN

Email: paul.hoffman@icann.org