Abstract

This document describes the DNS Security Extensions (commonly called "DNSSEC") that are specified in RFCs 4033, 4034, and 4035, as well as 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. A second purpose is to state that using DNSSEC for origin authentication of DNS data is the best current practice. A third purpose is to provide a single reference for other documents that want to refer to DNSSEC.

Status of This Memo

This memo documents an Internet Best Current Practice.

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 BCPs is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9364.

Copyright Notice

Copyright (c) 2023 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction
   1.1. DNSSEC as a Best Current Practice
   1.2. Implementing DNSSEC
2. DNSSEC Core Documents
   2.1. Addition to the DNSSEC Core
3. Additional Cryptographic Algorithms and DNSSEC
4. Extensions to DNSSEC
5. Additional Documents of Interest
6. IANA Considerations
7. Security Considerations
8. References
   8.1. Normative References
   8.2. Informative References
Acknowledgements
Author's Address

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 of DNS data. [RFC6840] updates and extends those core RFCs but does not fundamentally change the way that DNSSEC works.

This document lists RFCs that should be considered by someone creating an implementation of, or someone deploying, DNSSEC as it is currently standardized. Although an effort was made to be thorough, the reader should not assume this list is comprehensive. It uses terminology from those documents without defining that terminology. It also points to the relevant IANA registry groups that relate to DNSSEC. It does not, however, point to standards that rely on zones needing to be signed by DNSSEC, such as DNS-Based Authentication of Named Entities (DANE) [RFC6698].
1.1. DNSSEC as a Best Current Practice

Using the DNSSEC set of protocols is the best current practice for adding origin authentication of DNS data. To date, no Standards Track RFCs offer any other method for such origin authentication of data in the DNS.

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 websites are signed, and only around a third of queries to recursive resolvers are validated. However, this low level of deployment does not affect whether using 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 beneath some top-level domains (TLDs) and the near-universal deployment of DNSSEC for the TLDs in the DNS root zone demonstrate that DNSSEC is applicable 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 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 refer to as "DNSSEC" is the third iteration of the DNSSEC specification; [RFC2065] was the first, and [RFC2535] was the second. Earlier iterations have not been deployed on a significant scale. Throughout this document, "DNSSEC" means 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 about 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 a DNSSEC-aware authoritative server, and/or of a DNSSEC-aware recursive resolver from the three core documents, plus a few older RFCs specifying the cryptography used. Those two older documents are the following:

- [RFC2536] defines how to use the DSA signature algorithm (although it 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 among the most popular signing algorithms for DNSSEC.

It is important to note that later RFCs update the core documents. As just one example, [RFC9077] changes how TTL values are calculated in DNSSEC processing.

### 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 [RFC3155] as much a part of DNSSEC as NSEC is. It also makes the SHA-256 and SHA-512 hash functions defined in [RFC5155] and [RFC5702] part of the core.

### 3. Additional Cryptographic Algorithms and DNSSEC

Current cryptographic algorithms typically weaken over time as computing power improves and new cryptoanalysis emerges. Two new signing algorithms have been adopted by the DNSSEC community: Elliptic Curve Digital Signature Algorithm (ECDSA) [RFC6605] and Edwards-curve Digital Signature Algorithm (EdDSA) [RFC8624]. ECDSA and EdDSA have become very popular signing algorithms in recent years. The GOST signing algorithm [GOST-SIGN] 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, i.e., it is not advice about which algorithms zone operators should or should not use for signing, nor which algorithms recursive resolver operators should or should not use for validation.
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 the following:

- [RFC5011] describes a method to help resolvers update their DNSSEC trust anchors in an automated fashion. This method was used in 2018 to update the DNS root trust anchor.
- [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 maintenance 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 and NSEC3 for negative caching.
- [RFC9077] updates [RFC8198] with respect to the 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]. By generating and signing these records on demand, authoritative name servers can effectively stop the disclosure of zone contents otherwise made possible by walking the chain of NSEC records in a signed zone”.
- [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”. This background is particularly important for understanding NSEC and NSEC3 usage.
- [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”.
8. References

8.1. Normative References


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

6. IANA Considerations

IANA already has three registry groups that relate to DNSSEC:

- DNSSEC algorithm numbers
- DNSSEC NSEC3 parameters
- DNSSEC DS RRtype digest algorithms

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 registry groups or registries.

7. Security Considerations

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

8. References
8.2. Informative References


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 draft versions of this document: Ben Schwartz and Duane Wessels.
Author's Address

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