DNSOP
Internet-Draft
Intended status: Informational
Expires: January 4, 2018

D. York
Internet Society
O. Sury
CZ.NIC
P. Wouters
Red Hat
O. Gudmundsson
CloudFlare

July 3, 2017

Observations on Deploying New DNSSEC Cryptographic Algorithms
draft-york-dnsop-deploying-dnssec-crypto-algs-05

Abstract

As new cryptographic algorithms are developed for use in DNSSEC signing and validation, this document captures the steps needed for new algorithms to be deployed and enter general usage. The intent is to ensure a common understanding of the typical deployment process and potentially identify opportunities for improvement of operations.

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 http://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 January 4, 2018.

Copyright Notice

Table of Contents

1. Introduction

The DNS Security Extensions (DNSSEC), broadly defined in [RFC4033], [RFC4034] and [RFC4035], make use of cryptographic algorithms in both the signing of DNS records and the validation of DNSSEC signatures by recursive resolvers.

The current list of cryptographic algorithms can be found in the IANA "Domain Name System Security (DNSSEC) Algorithm Numbers" registry located at <http://www.iana.org/assignments/dns-sec-alg-numbers/> Algorithms are added to this IANA registry through a process defined in [RFC6014]. Note that [RFC6944] provides some guidance as to which of these algorithms should be implemented and supported.

Historically DNSSEC signatures have primarily used cryptographic algorithms based on RSA keys. As deployment of DNSSEC has increased there has been interest in using newer and more secure algorithms, particularly those using elliptic curve cryptography.

The ECDSA algorithm [RFC6605] has seen some adoption and the more recent [RFC8080] specifies the Edwards-curve Digital Signature Algorithm (EdDSA) using a choice of two curves, Ed25519 and Ed448.

The challenge is that the deployment of a new cryptographic algorithm for DNSSEC is not a simple process. DNSSEC algorithms are used throughout the DNS infrastructure for tasks such as:

- Generation of keys ("DNSKEY" record) for signing
- Creation of DNSSEC signatures in zone files ("RRSIG")
- Usage in a Delegation Signer ("DS") record [RFC3658] for the "chain of trust" connecting back to the root of DNS
- Generation of NSEC/NSEC3 responses by authoritative DNS servers
- Validation of DNSSEC signatures by DNS resolvers

In order for a new cryptographic algorithm to be fully deployed, all aspects of the DNS infrastructure that interact with DNSSEC must be updated to use the new algorithm.

This document outlines the current understanding of the components of the DNS infrastructure that need to be updated to deploy a new cryptographic algorithm.

It should be noted that DNSSEC is not alone in complexity of deployment. The IAB documented "Guidelines for Cryptographic Algorithm Agility" in [RFC7696] to highlight the importance of this issue.

1.1. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. Aspects of Deploying New Algorithms

For a new cryptographic algorithm to be deployed in DNSSEC, the following aspects of the DNS infrastructure must be updated:

- DNS resolvers performing validation
- Authoritative DNS servers

- Signing software
- Registries
- Registrars
- DNS Hosting Operators
- Applications

Each of these aspects is discussed in more detail below.

2.1. DNS Resolvers Performing Validation

DNS recursive resolvers perform "validation" to check the DNSSEC signatures of records received in a DNS query. To validate the signatures, the resolvers need to be able to understand the algorithm used to create the signatures.

In the case of a new algorithm, the resolver software needs to be updated. In some cases this could require waiting until an underlying library is updated to support the new algorithm.

Once the software is updated, the updates need to be deployed to all resolvers using that software. This can be challenging in cases of customer-premises equipment (CPE) that does not have any mechanism for automatic updating.

2.1.1. Resolvers and Unknown Algorithms

It should be noted that section 5.2 of [RFC4035] states:

> "If the resolver does not support any of the algorithms listed in an authenticated DS RRset, then the resolver will not be able to verify the authentication path to the child zone. In this case, the resolver SHOULD treat the child zone as if it were unsigned."

This means that signing a zone with a new algorithm that is not widely supported by DNS resolvers would result in the signatures being ignored and the zone treated as unsigned until resolvers were updated to recognize the new algorithm.

Note that in at least one 2016 case the resolver software deployed on customer premises by an Internet service provider (ISP) turned out not to be compliant with RFC 4035. Instead of ignoring the signatures using unknown algorithms and treating the zones as unsigned, the validating resolver rejected the signatures and

returned a SERVFAIL to the DNS query. This resulted in the ISP turning off DNSSEC validation on the equipment. Further investigation showed that a newer version of the resolver software did correctly support ECDSA, but now all customer premises equipment must be updated to this new version.

The point is that it is not safe to assume all resolver software will correctly implement this part of RFC 4035.

2.2. Authoritative DNS Servers

Authoritative DNS servers serve out signed DNS records. Serving new DNSSEC signing algorithms should not be a problem as a well-written authoritative DNS server implementation should be agnostic to the RR DATA they serve.

The one exception is if the new cryptographic algorithms are used in the creation of NSEC/NSEC3 responses. In the case of new NSEC/NSEC3 algorithms, the authoritative DNS server software would need to be updated to be able to use the new algorithms.

Note that some authoritative server implementations could include DNSSEC signing as part of the server and thus also fall into the "Signing Software" category below.

2.3. Signing Software

The software performing the signing of the records needs to be updated with the new cryptographic algorithm.

User interfaces that allow users to interact with the DNSSEC signing software may also need to be updated to reflect the existence of the new algorithm.

Note that the key and signatures with the new algorithm will need to co-exist with the existing key and signatures for some period of time. This will have an impact on the size of the DNS records.

One issue that has been identified is that not all commonly-used signing software releases include support for an algorithm rollover. This software would need to be updated to support rolling an algorithm before any new algorithms could be deployed.

2.3.1. NSEC3 Iterations

Implementation experience has shown that the [RFC5155] NSEC3 iteration count limits are poorly understood and are fragile in the context of adoption of elliptic curve(EC)-based algorithms.

A simple design would have constrained the iteration count only by the bit width of the iteration count field (perhaps 12 bits for up 4096 iterations), with all representable values supported by both signers and resolvers. Instead, the iteration count limit was made dependent on key size. When the original text of Section 10.3 of [RFC5155] was written, the only commonly used DNSSEC key algorithms were RSA and DSA. These had similar key sizes with comparable security, with DSA slower than RSA. A decision was made to specify iteration count limits roughly commensurate with the cost of RSA operations for a given key size, and to use the same limits for both RSA and DSA. The essential features of the specification are:

> The limits, therefore, are based on the size of the smallest zone signing key, rounded up to the nearest table value (or rounded down if the key is larger than the largest table value).
> ...
> Therefore the values in the table MUST be used independent of the key algorithm.

While the specified key-size-dependent limits made some sense for both RSA and DSA, they map poorly to elliptic-curve-based (EC) DNSSEC algorithms, which only use keys shorter than 1024 bits. Nevertheless, popular DNS resolvers apply the specified table of limits to EC algorithms, and so zones with EC keys need to cap their NSEC3 iteration counts at 150.

This requirement is surprising to some operators migrating from RSA to EC keys. They continue to use iteration counts that work for RSA-2048, but which exceed the 150 limit for the smaller EC keys. This renders denial-of-existence "Insecure" for the zones in question.

Some signer implementations allow maximums that are higher than the specified key-size-dependent limits, resulting again in resolvers possibly returning these answers as "Insecure".

To avoid surprises, such as downgrade attacks against "SMTP Security via Opportunistic DANE TLS" [RFC7672], DNSSEC signers should not use an iteration count higher than 150: such iteration counts are prone to fail when configuration changes introduce new algorithms.

Similarly, resolvers should not support configurations with iteration count limits below 150, as lower limits may lead to insecure denial of existence, even for compliant zones.

2.4. Registries

The registry for a top-level domain (TLD) needs to accept DS records using the new cryptographic algorithm.

Observations to date have shown that some registries only accept DS records with certain algorithms. Registry representatives have indicated that they verify the accuracy of DS records to reduce technical support incidents and ensure customers do not mistakenly create any outages.

However, this means that registries who perform this level of checking must be able to understand new algorithms in order to successfully verify the DS records.

Separately, feedback from registrars has indicated that they do not currently have any mechanism to understand what DNSSEC algorithms a registry can accept.

2.5. Registrars

Registrars perform a critical role in the DNSSEC "chain of trust" of passing the DS record up to the Registry to ensure that the signed zone can be authenticated from the root of DNS all the way to the zone.

If the registrar is also providing the DNS hosting services for a domain, the registrar can easily create the "DS" record from the "DNSKEY" record and pass the DS record up to the registry.

However, if the authoritative servers for a domain are not with the registrar, then the registrar needs to provide some mechanism to accept a DS record to pass that up to the registry. Typically this is done through a web interface.

An issue is that many registrar web interfaces only allow the input of DS records using a listed set of DNSSEC algorithms. Any new cryptographic algorithms need to be added to the web interface in order to be accepted into the registrar's system.

Additionally, in a manner similar to registries, many registrars perform some level of verification on the DS record to ensure it was entered "correctly". To do this verification, the registrar's software needs to understand the algorithm used in the DS record. This requires the software to be updated to support the new algorithm.

Note that [RFC8078] defines an automated mechanism to update the DS records with a registry. If this method becomes widely adopted, registrar web interfaces may no longer be needed.

2.6. DNS Hosting Operators

DNS hosting operators are entities that are operating the authoritative DNS servers for domains and with DNSSEC are also providing the signing of zones. In many cases they may also be the registrar for domain names, but in other cases they are a separate entity providing DNS services to customers.

DNS hosting operators need to update their authoritative DNS server software to understand new cryptographic algorithms, but they also need to update their web interfaces and provisioning software to allow configuration and support of new algorithms.

2.7. Applications

Beyond the recursive resolvers, authoritative servers, web interfaces and provisioning software, it has been observed that some applications (or "apps"), particularly in the mobile environment, are including their own DNS resolvers within the app itself. These recursive resolvers are used by the app instead of the recursive resolver included with the underlying operating system. These applications that perform DNSSEC validation would need to also be updated to understand a new algorithm.

In many cases, it may be that an underlying developer library needs to be updated first. It will then depend upon how long it takes the application developer to pull in the updated library.

Outside of applications, these developer libraries are also typically used by recursive resolver software and signing software.

3. Conclusion

This document provides a view into the steps necessary for the deployment of new cryptographic algorithms in DNSSEC at the time of this publication. In order to more rapidly roll out new DNSSEC algorithms, these steps must be understood and hopefully improved over time.

It should be noted that a common theme to emerge from all discussions is a general reluctance to update or change any DNS-related software. "If it isn't broken, don't fix it" is a common refrain. While perhaps understandable from a stability point of view, this attitude creates a challenge for deploying new algorithms.

One potential idea suggested during discussions was for some kind of web-based testing tool that could assist people in understanding what algorithms are supported by different servers and sites.

It is also quite clear that any deployment of new algorithms for DNSSEC use will take a few years to propagate throughout the infrastructure. This needs to be factored in as new algorithms are proposed.

4. IANA Considerations

This document does not make any requests of IANA.

5. Security Considerations

No new security considerations are created by this document.

It should be noted that there are security considerations regarding changing DNSSEC algorithms mentioned in both [RFC6781] and [RFC7583].

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc4035>.

[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, <http://www.rfc-editor.org/info/rfc5155>.

[RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)", RFC 7672, DOI 10.17487/RFC7672, October 2015, <http://www.rfc-editor.org/info/rfc7672>.

[RFC8078] Gudmundsson, O. and P. Wouters, "Managing DS Records from the Parent via CDS/CDNSKEY", RFC 8078, DOI 10.17487/RFC8078, March 2017, <http://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, <http://www.rfc-editor.org/info/rfc8080>.

6.2. Informative References

[RFC3658] Gudmundsson, O., "Delegation Signer (DS) Resource Record (RR)", RFC 3658, DOI 10.17487/RFC3658, December 2003, <http://www.rfc-editor.org/info/rfc3658>.

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

[RFC6605] Hoffman, P. and W. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, DOI 10.17487/RFC6605, April 2012, <http://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, <http://www.rfc-editor.org/info/rfc6781>.

[RFC6944] Rose, S., "Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status", RFC 6944, DOI 10.17487/RFC6944, April 2013, <http://www.rfc-editor.org/info/rfc6944>.

[RFC7583] Morris, S., Ihren, J., Dickinson, J., and W. Mekking, "DNSSEC Key Rollover Timing Considerations", RFC 7583, DOI 10.17487/RFC7583, October 2015, <http://www.rfc-editor.org/info/rfc7583>.

[RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015, <http://www.rfc-editor.org/info/rfc7696>.

Appendix A. Acknowledgements

The information in this document evolved out of several mailing list discussions and also through engagement with participants in the following sessions or events:

- DNSSEC Workshop at ICANN 53 (Buenos Aires)
- DNSSEC Workshop at ICANN 55 (Marrakech)
- Spring 2016 DNS-OARC meeeting (Buenos Aires)
- various IETF 95 working groups (Buenos Aires)
- Panel session at RIPE 72 (Copenhagen)
- DNSSEC Workshop at ICANN 56 (Helsinki)

The authors thank the participants of the various sessions for their feedback.

The authors thank Viktor Dukhovni for contributing the text for the section on NSEC3 Iterations.

Appendix B. Changes

NOTE TO RFC EDITOR - Please remove this "Changes" section prior to publication. Thank you.

- Revision -05 corrected typos around two other references that did not appear in -04. It also added the new section on "NSEC3 Iterations" contributed by Paul Wouters and Viktor Dukhovni.
- Revision -04 corrected the references which did not appear in -03 due to an error in the markdown source.
- Revision -03 removed the reference to the location of the ISP in the text added in version -02.
- Revision -02 added text to the resolver section about an example where resolver software did not correctly follow RFC 4035 and treat packets with unknown algorithms as unsigned. The markdown

source of this I-D was also migrated to the markdown syntax favored by the 'mmark' tool.

- Revision -01 adds text about authoritative servers needing an update if the algorithm is for NSEC/NSEC3. Also expands acknowledgements.

Authors' Addresses

Dan York
Internet Society

Email: york@isoc.org
URI: https://www.internetsociety.org/

Ondrej Sury
CZ.NIC

Email: ondrej.sury@nic.cz

Paul Wouters
Red Hat

Email: pwouters@redhat.com

Olafur Gudmundsson
CloudFlare

Email: olafur+ietf@cloudflare.com