DNSSEC Algorithm Use in 2022

ICANN Office of the Chief Technology Officer

Paul Hoffman
OCTO-033
4 April 2022

TABLE OF CONTENTS

This document is part of ICANN's Office of the Chief Technical Officer (OCTO) document series. Please see the OCTO publication page for a list of documents in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

This document supports ICANN's strategic goal to improve the shared responsibility for upholding the security and stability of the Domain Name System (DNS) by strengthening DNS coordination in partnership with relevant stakeholders. It is part of ICANN's strategic objective to strengthen the security of the DNS and the DNS root server system (RSS).

1 Introduction

This document gives a brief overview of the algorithms, key sizes, and other options used in DNSKEY records in the DNS near the beginning of 2022. There has been some interest in the technical community about this information, so ICANN's OCTO team collected the data, analyzed it, and are reporting it here in case the analysis is useful. Given that it is the first such report from ICANN, and given the informal nature of the data collection, it is not meant to show any particular operational trends.

2 How the Data Was Collected

Any survey of the zones in the DNS will inherently be incomplete because the DNS does not have a method for searching for all known records. However, there are some good starting points in order to perform research into possibly representative names in the DNS.

This report draws from five sources:

- All the data in every generic top-level domain (gTLD) zone, similar to what is available to researchers from ICANN's Centralized Zone Data Service (CZDS). Each domain name with one or more delegation signer (DS) records in any of these gTLD zone files was queried for the associated DNSKEY records.
- Zone files made publicly available from a few country code top-level domain (ccTLD) operators. At the current time, these are the zones for .se and .nu (provided by Internetstiftelsen), and for .ch and .li (provided by SWITCH). Each domain name with a DS record in any of these four ccTLD zone files was then queried for the associated DNSKEY records.
- Domain names that appear on pages in the approximately 750 different Wikipedia sites. See "Collecting 'Typical' Domain Names for Web Servers," OCTO-023, for information on how these names were extracted from the open Wikipedia dataset.
- The complete list from the Tranco top sites database. This database collects the "top sites" list from other sources and combines them in a way that reduces the chance of manipulation.
- The 50 million highest ranked names from Common Crawl, which is an open repository of web crawl data.

The Wikipedia, Tranco, and Common Crawl data are domain names extracted from URLs found on the web. Each of these domain names was queried for associated DNSKEY records, although only a very small percentage of the names had them.

The result was a list of approximately 18.7 million DNSKEY records. This is definitely just a subset of all the DNSKEY records in the DNS. Other researchers use different methods to find and analyze DNSKEY records; for example, see "DNSSEC and DANE Deployment Statistics" for an analysis using a different aggregation methodology and a larger set of DNSKEY records that leads to different numeric results.

3 Signing Algorithms, RSA Key Sizes, and Key Flags

The significant algorithms used in the DNSKEY records in the dataset were:

RSA-SHA256	65.2%
ECDSA-P256-SHA256	30.5%
RSA-SHA1	2.0%
RSA-SHA512	1.1%
RSASHA1-NSEC3-SHA1	0.8%
ECDSA-P384-SHA384	0.4%

The other algorithms (such as EdDSA and GOST) had less than 0.1% of the signature algorithms seen.

Signing algorithms in DNSSEC that use RSA cryptography allow for any key sizes. For the RSA algorithms above, the significant key sizes were:

512 bits	0.1%
1024 bits	45.1%
1280 bits	0.1%
2048 bits	51.4%
4096 bits	0.7%

Many key sizes (such as 1536 and 3072) with less than 0.1% of the share were also seen.

The flags on the DNSKEY records indicate that almost exactly half of the keys are used as key-signing keys (KSKs), and the other half as zone-signing keys (ZSK). There is a significant difference in the RSA key lengths between KSKs and ZSKs:

	1024 bits	2048 bits	4096 bits
KSK	0.2%	98.6%	1.0%
ZSK	82.7%	11.9%	0.4%

4 Errors

In looking at the long tails in the collected data, it was quite easy to find values in use that create a danger of easy spoofing, that prevent the validation of signatures, or that are harmless typos.

RSA key sizes 768 bits or less are clearly dangerous, and they have been for over a decade. The fact that even 0.1% of the RSA keys have such dangerous sizes shows that the key generation software does not prevent the creation of too-short keys, which it very likely should do.

Some of the errors that were seen caused the published keys to be unusable. For example, about 2.6% of RSA keys have 600-bit exponents that appear to contain ASCII text; these are likely due to software errors because validating signatures with these keys would be onerous. Similarly, a small number of the keys seen have algorithm flags that make no sense.

A very small number of the keys found use an RSA exponent of 65337 instead of the near-universally used 65537. This is not dangerous because there is no indication that picking any correctly-formed RSA exponent will result in a breakable key as long as the exponent is not too large.

5 Conclusion

This document is simply a collection of observations, not an analysis of those observations. The dataset used is known to be a subset of the DNSKEY records in the DNS, but it cannot be determined if this subset is representative of the DNS as a whole.

Repeating the data collection in the future would show trends. The balance between RSA-SHA256 and ECDSA-P256-SHA256 may shift, or perhaps the other elliptic curve algorithms might see noticeable increases. Zone operators who stay with RSA are likely to switch from 1024 bits to 2048 bits over time, although the rate of change cannot be predicted.