State of DNSSEC Deployment 2016

December 2016

Internet Society

Executive Summary

This report provides a snapshot of the state of deployment of DNSSEC as of the end of 2016. Highlights:

- Signing of domains with DNSSEC:
  - 89% of top-level domains (TLDs) zones signed.
    - ~47% of country-code TLDs (ccTLDs) signed.
  - Second-level domains (SLDs) vary widely:
    - Over 2.5 million .nl domains signed (~45%) (Netherlands).[1]
    - ~88% of measured zones in .gov are signed.
    - Over 50% of .cz (Czech Republic) domains signed.
    - ~24% of .br domains signed (Brazil).[2]
    - While only about 0.5% of zones in .com are signed, that percentage represents ~600,000 zones.
  - The major DNS authoritative server software and libraries support DNSSEC and have several years of deployment experience.
  - Management tools have started to come online to assist deployment, e.g., key deployment and rollover.
  - Encryption algorithms and key lengths
    - The overwhelming majority of TLDs utilize RSA/SHA-256 with 2048 bit keys for the Key Signing Key (KSK) and 1024 bit keys for the Zone Signing Key (ZSK).
    - A significant number of zones measured still utilize SHA-1.
    - Utilization of ECDSA is at 5% and growing.
  - In 2016, the Zone Signing Key (ZSK) for the Root Zone was successfully migrated to a 2048-bit RSA key.
  - 2017 will be an important year for DNSSEC with the planned rollover of the Key Signing Key (KSK) in the Root Zone of DNS.

[1] https://www.dnssec.nl/home.html

[2] http://registro.br/estatisticas.html

- Validation
    - All major DNS recursive resolvers support DNSSEC validation.
    - ~80% of clients request DNSSEC digital signature records in their DNS queries (per APNIC research).
    - 26% of end user environments use DNSSEC-validating resolvers, but also pass queries to non-validating resolvers if validation results in a validation failure.
    - Although only ~14% of clients globally exclusively use DNSSEC-validating DNS resolvers, the numbers vary greatly between regions and countries.
        - Over 50% of clients in most Scandinavian countries exclusively use DNSSEC-validating DNS resolvers.
    - A large ISP enabling DNSSEC validation on its recursive resolvers can have a big impact on a country's utilization numbers (e.g. Comcast in USA, Claro in Brazil).
    - Google Public DNS (PDNS) service support for DNSSEC validation makes validation available globally (where allowed by law).
- Applications/Services
    - Libraries, APIs and tools are becoming available to enable DNSSEC use by application developers.
    - DANE
        - Utilization of DANE is relatively low, but growing.
        - Libraries, APIs and tools are becoming available.
        - Most prominent utilization of DANE is securing email transfers between email servers, led by German email providers.

In summary, deployment of DNSSEC has made substantial progress since the root was signed in 2010. Most of the Top Level Domains (TLDs) have now been signed (with some challenges in ccTLDs, especially in developing countries). The major DNS servers and resolvers now ship with DNSSEC capability, and tools assisting DNSSEC operation are improving. New applications for DNSSEC, such as the use of DANE for securing email transfers, are gaining traction. While there are still challenges in deploying and supporting DNSSEC, the above factors point to continued growth.

Table of contents

Executive Summary....2

1 Introduction....5

2 State of DNSSEC Validation....7

2.1 Observed usage of DNSSEC validation....7

2.2 Availability of DNSSEC validation in DNS resolver software....11

3 State of DNSSEC Signing....13

3.1 Top-Level Domains....14

3.2 Second-level domains (SLDs)....17

3.3 Algorithms and key sizes....22

4 State of Deployment of DNS-based Authentication of Named Entities (DANE)....25

5 Root Key Signing Key (KSK) Rollover....29

6 Challenges to Deployment....30

6.1 Challenges with changing cryptographic algorithms....30

6.2 Case study - Elliptic Curve Digital Signature Algorithm (ECDSA) rollout 32

6.3 Automation of secure delegations....34

7 Conclusion....35

8 References....36

9 Appendix: Resources....39

10 Acknowledgements....39

1 Introduction

In the almost 20 years since the publication of RFC 2065, "Domain Name System Security Extensions" [RFC2065] in January of 1997, the DNS security extensions (DNSSEC) have been implemented, tested, deployed and updated [RFC4033][RFC4034][RFC4035]. New capabilities have been defined, such as the DNS-Based Authentication of Named Entities (DANE)[RFC6394]. Like IPv6, DNSSEC deployment has faced challenges due to technology issues and lack of motivation. Operational deployment was very slow until Dan Kaminsky's disclosure of a serious cache poisoning attack in 2008 [KAMINSKYBUG] stimulated renewed interest in DNSSEC. The signing of the root zone in 2010 provided a firm basis for DNSSEC deployment by enabling a chain of trust up to the DNS root. Since 2010, deployment of DNSSEC in the Top Level Domain (TLD) zones and Second Level Domains [SLD] has progressed.

The Internet Society (ISOC) launched its Deploy360 Programme in 2011 including its web portal supporting deployment of DNSSEC[3]. The Deploy360 Programme provides information on and links to training, tools, case studies and deployment statistics to assist and track the deployment of DNSSEC.

There are two main aspects of deployment of DNSSEC addressed in this report:

- **DNSSEC signing**
    - How many zones are signed using DNSSEC and have a chain of trust back to the DNS root?
    - What algorithms and key sizes are supported?
- **DNSSEC validation**
    - What recursive resolvers support DNSSEC?
    - How many clients are using DNSSEC-validating DNS resolvers?

With DANE, the Internet Engineering Task Force (IETF) has defined a way to use the chain of trust provided by DNSSEC in authenticating

[3] http://www.internetsociety.org/deploy360/dnssec/

certificates used in Transport Layer Security (TLS, more commonly known by the historic name of Secure Socket Layer or "SSL") [RFC6698][RFC7671]. Section 4 looks at the state of deployment of DANE on the Internet. Similar to DNSSEC, deployment is viewed from two angles:

- Signing – how many sites provide TLSA records in DNS.
- Utilization – How many and what types of applications/services use TLSA records in establishing TLS Sessions.

Given the impact that the root Key Signing Key rollover has on the DNS, Section 5 provides a short discussion of the status of the current KSK rollover process.

Section 6 describes some of the main challenges to deployment including an overview of those facing migration to a new crypto algorithm (e.g., Elliptic Curve Digital Signature Algorithm (ECDSA)).

While deployment of DNSSEC has historically been slow, the signing of the root zone and most of the TLD zones, widespread support in DNS server and recursive resolver software, increasing availability of tools for deployment and new applications and services (e.g., DANE) have driven increased growth over the last 5 years.

2 State of DNSSEC Validation

Once a zone is cryptographically signed with a chain of trust to the root zone, including the requisite RRSIG, DNSKEY, NSEC/NSEC3 and DS records, DNS resolvers can use these records and public key cryptography to validate information returned in response to a DNS query. Because of the increased response size due to these additional records, the resolver also must be able to support the Extension Mechanisms for DNS (EDNS0)[RFC6891].

Measuring the state of DNSSEC validation is qualitatively and quantitatively different than measuring the signed zones (e.g., TLDs). For signed zones, the relevant Resource Records are relatively static (modulo dynamic DNS), is in a relatively well-known location (authoritative name server) and the cases tend to be limited. For validation, there are multiple points of measurement (e.g., at DNS server, multiple levels of recursive resolvers, at client) with many failure modes. As examples, a recursive resolver might request DNSSEC RRs but not actually validate the response or a client might receive a SERVFAIL response from a validating recursive resolver and fall back to a non-validating secondary resolver. In addition, there can be multiple levels of recursive resolvers and forwarders, which can obscure where validation is being done.

2.1 Observed usage of DNSSEC validation

The best publicly available ongoing measurements on DNSSEC validation are currently being collected by APNIC. The APNIC statistics measure clients that exclusively use DNSSEC validating name resolution (either directly or via a validating recursive resolver)[APNICM]. Figure 1 illustrates the state of DNSSEC validation as measured by APNIC as of 18 December, 2016.

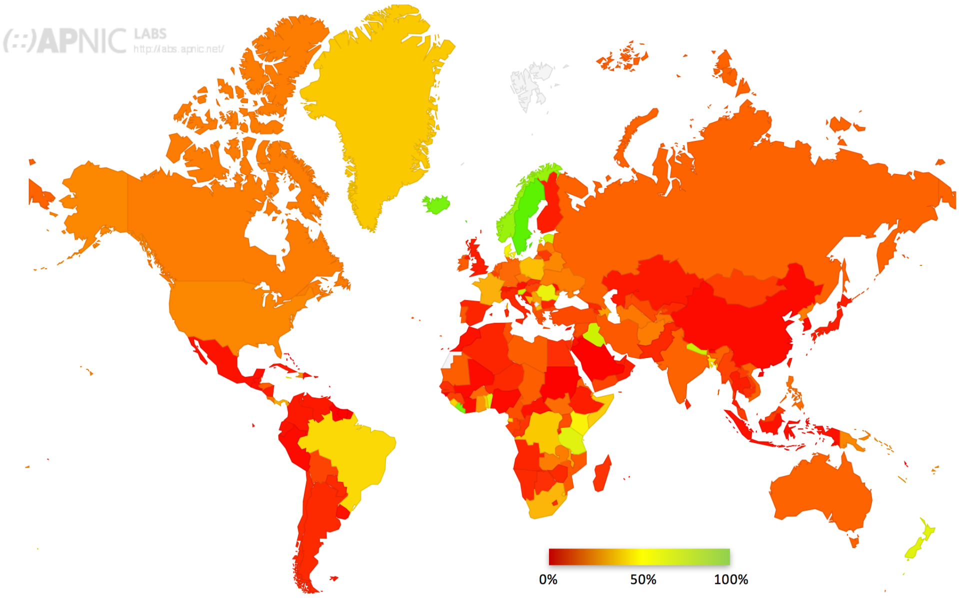

Figure 1 - Global State of DNSSEC Validation[4]

APNIC also keeps track of the percentage of clients that query Google's Public DNS service (PDNS)[5]. Since Google PDNS supports DNSSEC validation, any client that uses the service will have access to DNSSEC validation. In some cases, ISPs point their customers to Google PDNS to use as DNS recursive resolvers instead of providing their own. As described in the DNSSEC Workshop in ICANN56, the effect can be seen in the relatively high usage of DNSSEC in central Africa which uses Google's PDN services (e.g., 77% of clients in the Democratic Republic of the Congo utilize Google PDNS).[6]

As shown in Figure 1 and Table 1, support for DNSSEC validation is not distributed evenly across the regions. Deployment in Asia is only half that in Europe, Americas and Oceania (but makes up over half the samples taken). Within Europe, Scandinavian countries stand out in their native (non-Google PDNS) support for DNSSEC validation.

Figure 2 illustrates the global growth in DNSSEC validation since 2014, when APNIC started its measurements. These measurements indicate that ~14% of DNS queries currently support DNSSEC validation up from 8-9%

[4] http://stats.labs.apnic.net/DNSSEC

[5] https://developers.google.com/speed/public-dns/

[6] Geoff Huston, DNSSEC Workshop, ICANN56, https://icann562016.sched.org/event/7NCj/dnssec-workshop-part-1.

support in 2014. As can be seen, growth in DNSSEC validation started to level off globally in 2016.

Growth in validation is not necessarily gradual on a per-country basis. The numbers can jump substantially based on a large ISP turning on DNSSEC validation in its customer-facing resolvers. For example, Figure 3 illustrates how DNSSEC validation in Brazil jumped approximately 10% when Claro turned on DNSSEC validation in its customer-facing resolvers in April-May 2015[7]. Although occurring before APNIC started its measurements, Comcast in the US effected a similar jump in validation when it turned on DNSSEC validation for its ~18 million customers.

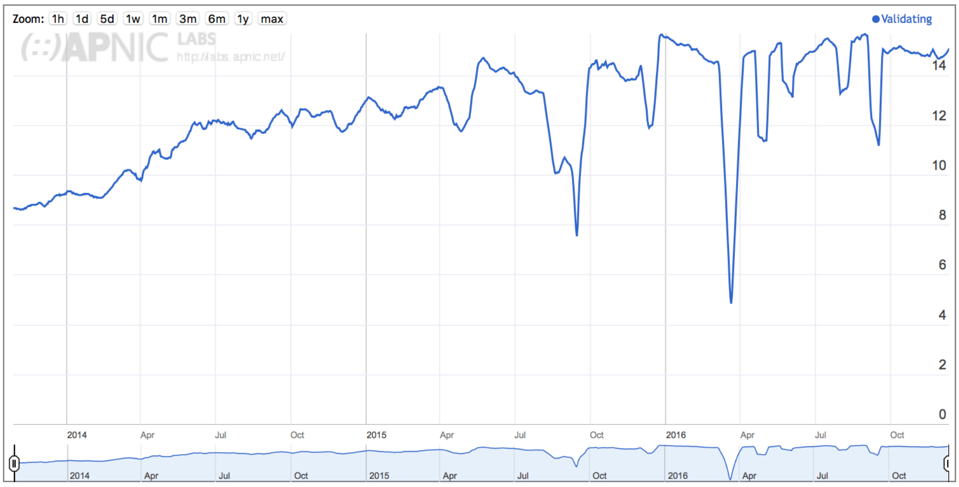

Figure 2 - Growth of DNSSEC Validation Globally[8][9]

[7] Ibid.

[8] http://stats.labs.apnic.net/dnssec/XA?c=XA&x=1&g=1&r=1&w=1&g=0 (12/13/2016) with 14 day interval

[9] The notches in the graph are artifacts from the measurement technique used.

Region	DNSSEC Validates	Uses Google PDNS
World	14.95%	14.16%
Oceania	23.80%	5.61%
Americas	22.50%	12.88%
Europe	20.02%	9.33%
Africa	16.58%	28.61%
Asia	10.17%	13.11%

Table 1 - Regional DNSSEC Validation

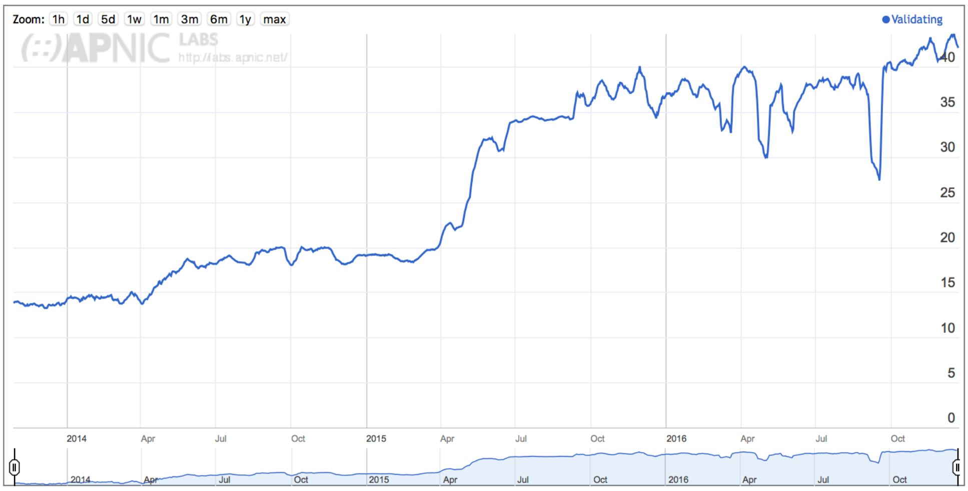

Figure 3 - Use of DNSSEC Validation for Brazil[10]

In Figures 2 and 3, the y-axis represents the percentage of clients exclusively using validating resolvers. APNIC's experiment also show a difference in numbers in how DNSSEC is deployed. While APNIC's measurements found that ~80% of queries requested DNSSEC credentials, only 26% perform DNSSEC validation on the returned credentials and ~11% of the clients fall back to a non-validating resolver on receipt of a SERVFAIL response. This leaves the ~15% of clients that fully utilize DNSSEC validation (fail on SERVFAIL).[11]

[10] https://stats.labs.apnic.net/dnssec/BR?c=BR&x=1&g=0&r=1&w=14 (14 day interval)

[11] Geoff Huston, DNSSEC Workshop, ICANN56, https://icann562016.sched.org/event/7NCj/dnssec-workshop-part-1.

2.2 Availability of DNSSEC validation in DNS resolver software

One of the complaints against DNSSEC has been the lack of availability of DNSSEC-capable resolvers. While this might have been true several years ago, there are currently many options for DNSSEC validation support. Table 2 provides a partial list of DNS resolvers or resolution services that support DNSSEC and Table 3 lists the availability of software libraries for developers needing to use DNSSEC queries."

Vendor/ Developer	Resolver (Caching, Recursive)	Type	Comment
BT	Diamond IP/SX20	P	http://www.globalservices.bt.com/us/en//products/diamondip_dnssec
Cisco	Prime Network Registrar (DDI)	P	http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-network-registrar/white-paper-c11-730186.html Unbound
Infoblox	Infoblox (DDI)	P	
ISC	BIND	OSS	At least 9.6
NLnet Labs	Unbound	OSS	
Secure64®	DNS Cache	P	http://www.secure64.com/fast-secure-DNS-caching http://www.secure64.com/library/documents/Datasheets/DNS-Cache-Datasheet.pdf
Google	Public DNS	Sv	Homegrown – Resolution service
Nominum	Vantio™ Cacheserve	Sv	
PowerDNS	PowerDNS Recursor	P	> v4.0.0 for validation
Microsoft	Windows Server	P	
CZ.NIC	Knot DNS Resolver	OSS	https://www.knot-resolver.cz/
Simon Kelley	dnsmasq	OSS	http://www.thekelleys.org.uk/dnsmasq/doc.html
P Sv OSS	Commercial Product Resolver Service Open Source Software		

Table 2 - DNSSEC capable resolvers and resolution services

Language	Library	Comment
C	getDNS	a newer project to provide a more modern API for DNS
	ldns from NLnet Labs	
	libval from the DNSSEC-Tools Project	
	libunbound, a component of the Unbound DNS resolver that can be used in other applications	
Erlang	dns_erlang	
Go	godns	
Java	dnsjava	
	DNSSEC4J	(based on the DNSSEC primitives in dnsjava)
	Dnssecjava	A DNSSEC validating stub resolver for Java.
Perl	Net::DNS and Net::DNS::SEC	
	Perl modules from the DNSSEC-Tools Project	
Python	dnspython	Also available on Github
	python-dnssec	
	PyUnbound	a python wrapper for the libunbound library (mentioned above under C)
Ruby	dnsruby	
Object(?)	Bind 9 libraries	BIND 9 export libraries
C#/.Net	ARSoft.Tools.Net	C#/.Net DNS client/server, SPF and SenderID Library https://arsofttoolsnet.codeplex.com
PHP	Net_DNS2	Native PHP5 DNS Resolver and Updater
Other	Google DNS-over-HTTPS API	HTTPS API using Googles Public DNS. Responses are in JSON.

Table 3 - DNS Developer Libraries

3 State of DNSSEC Signing

The signing of DNS zones and associated chain of trust to the root is the heart of DNSSEC, enabling validation. This section does not address all corner cases (e.g., having a subset of RRsets signed, chain of trust not rooted in the DNS root zone). The hierarchical nature of the DNS carries over to DNSSEC where the chain of trust requires valid signing of zones from the target zone all the way up to the root. If a higher-level zone is not signed, then its child zones will not be able to establish a chain of trust even if they are signed.

For the purposes of this document, a zone is considered to be signed by DNSSEC if the following are true:

- In the zone:
    - Existence of at least one DNSKEY RR for a ZSK and a KSK[12] for the zone.
    - Existence of RRSIG RRs for the RRsets in the zone signed by one of the ZSKs.
    - Existence of RRSIG Records for the DNSKEY RRset signed by the KSK if different keys are used for the ZSK and KSK function.
- In the parent zone:
    - Existence of a DS Record for the zone's KSK.
    - Existence of an RRSIG for the DS Record for the zone signed by the ZSK of the parent zone.
- Chain of trust (DS RRs) to the DNS root signing key

In 2010, the DNS root zone was signed enabling a chain of trust anchored in the DNS root. This allowed TLD operators to start signing their zones and placing their DS Records in the root. This, in turn, enabled Second Level Domain operators to start signing their zones, and so on down the chain.

Starting in 2012, ICANN required applications for new generic TLDs (gTLDs)[13] to support DNSSEC from the start. ICANN also updated its

[12] Note: A single DNSKEY RR could contain a ZSK and KSK, but general practice is that they are separate.

[13] For the purpose of this document, we include "sponsored" and "restricted" TLDs as part of "generic TLDs".

Registrar Accreditation Agreement in 2013 to require registrars to allow customers to use DNSSEC (if supported by the underlying Registry). These actions enabled an increased number of zone operators to sign their zones with a chain of trust to the DNS root. Note that the 2012 requirement on new gTLDs to support DNSSEC does not apply to ccTLDs. Neither the 2012 nor the 2013 requirement apply to previous gTLDs or registrars operating under earlier agreements. This helps explain the jump in TLD zone signing in 2013 and the disparity between the gTLDs and ccTLDs in signing their zones. Although not required by the above agreements, the gTLDs created prior to 2012 have almost all signed their zones (two exceptions being .tel and .aero).

Signing of Second Level Domain (SLD) zones (and their child zones) is generally left up to the zone operator(s).

Section 3.1 provides the current status of signing TLDs including ccTLDs and gTLDs. Section 3.2 provides information on the status of Second Level Domains (SLDs).

3.1 Top-Level Domains

According to ICANN's statistics, as of November, 2016 (see Table 4) 89% of all TLDs have signed their zones and have a Delegation Signer (DS) resource record (RR) in the DNS root. Another 1% have signed their zones but have not added a DS RR to the root, and 10% of TLDs have not signed their zones.

Breaking these numbers down further we can see that 100% of the current gTLDs are signed with a DS RR in the root, including all internationalized gTLDs. Based on the 2012 ICANN requirement on new gTLDs all future gTLDs should also be signed from the start.

The country-code TLDs (ccTLD) have the most room for improvement. As of November 2016 only 47% of ccTLDs are signed with a DS RR in the root zone. ICANN does not have any requirement on ccTLDs to sign their zones and due to national sovereignty concerns it is doubtful there will ever be such a requirement. Thus it is up to each ccTLD operator to determine if it will sign the zone for its country. The map in Figure 4 illustrates the status of DNSSEC signing of ccTLDs globally.

	Total	Signed[14]		Signed w/DS in Root		Unsigned	
		Count	%	Count	%	Count	%
All TLDs	1518	1369	90.2%	1358	89%	149	9.8%
ccTLDs	294	148	50.3%	138	47%	146	49.7%
gTLDs	1223	1220	99.8%	1219	100%	3	0.2%

Table 4 - DNSSEC signed TLDs

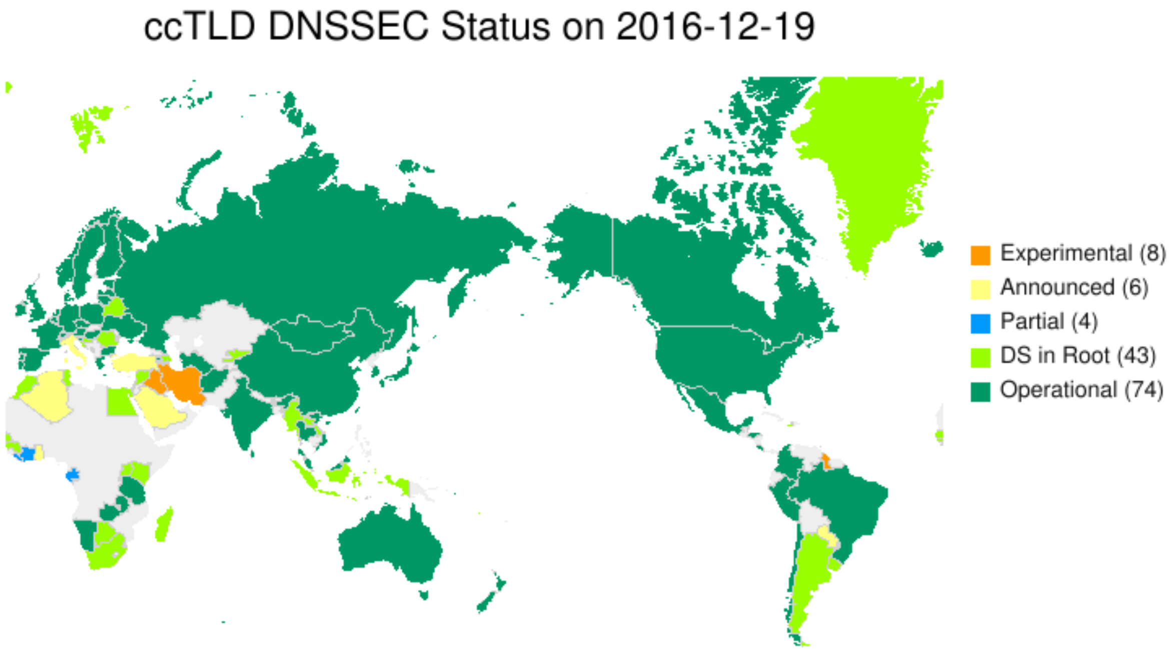

Figure 4 - ccTLD DNSSEC Status on 2016-12-19[15]

Figure 5 through Figure 7 show the growth in signing of TLDs since 2010 (ICANN statistics). They illustrate the rapid growth in gTLDs starting in 2013. The growth of signing of ccTLDs has been slow but steady.

[14] Includes TLDs that are signed but don't have a DS RR in the root zone.

[15] Deployment maps published weekly at http://www.internetsociety.org/deploy360/dnssec/maps/

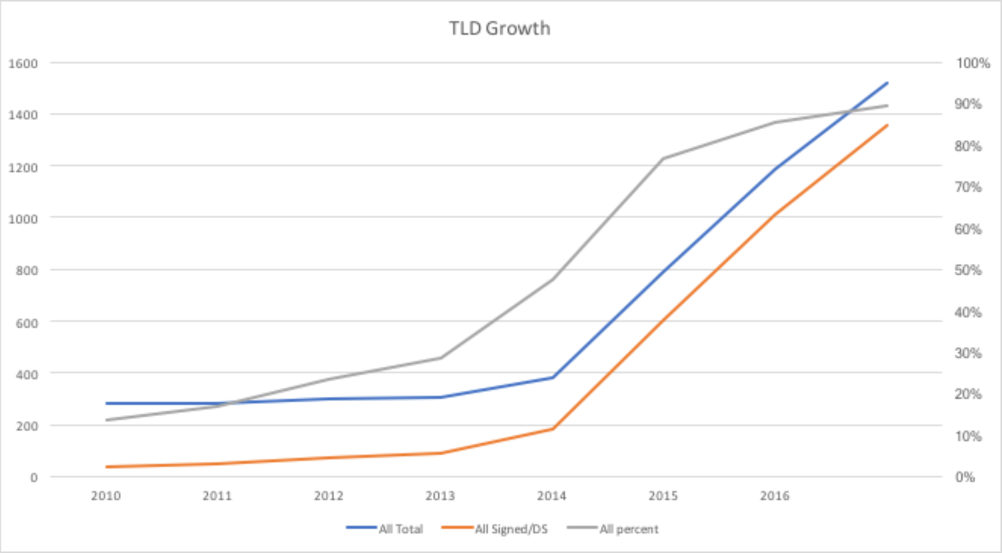

Figure 5 - Growth of Signed TLDs

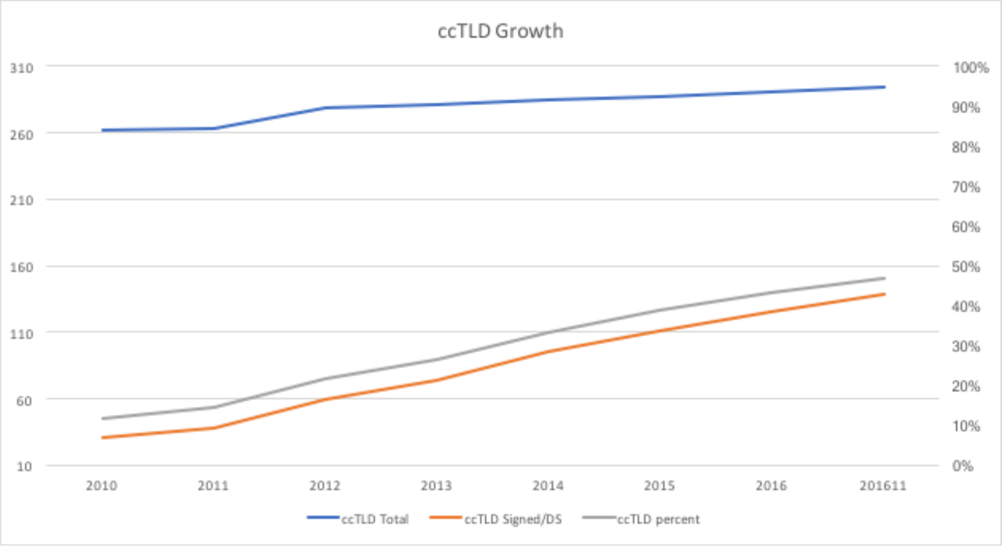

Figure 6 - Growth of Signed ccTLDs

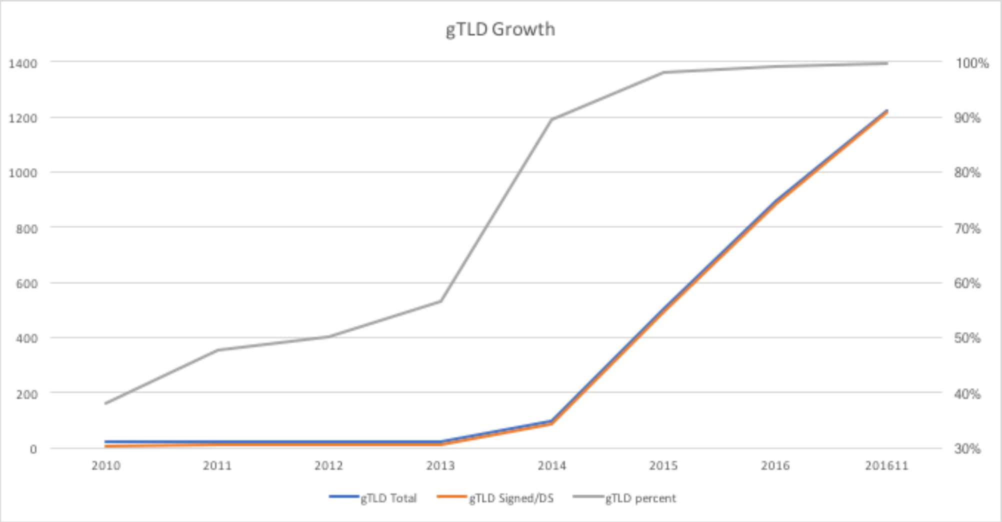

Figure 7 - Growth in Signed gTLDs

3.2 Second-level domains (SLDs)

Statistics for signing of SLDs (and below) are more difficult to track with the same accuracy and consistency as TLDs, due to the large number of zones and their dynamics. The different efforts to measure the status of signing of zones below the TLD level can show different numbers based on what criteria they are using, where they are polling from, the polling interval and time, etc.

Verisign Labs' SecSpider effort measures a set of approximately 2 – 2.5 million zones collected from different sources (e.g., volunteered data, zones crawled via polling systems, walking zones via NSEC). Table 5 shows the current numbers.[16]

[16] http://secspider.verisignlabs.com/stats.html (23 December 2016)

1,949,282	Zones monitored
1,629,021	DNSSEC enabled zones
1,621,499	Zones use both KSKs and ZSKs
176	Zones are serving revoked keys
1,525,050	DNSSEC verified zones

Table 5 - DNSSEC Signed Zones

The SecSpider effort considers a zone secure if it meets the following criteria:

- Must support EDNS0
- Must have RRSIG records attached to resource record sets (RRsets)
- Must *not* have a CNAME for the zone's domain name
- Must provide NSEC records for denial of existence

Figure 8 illustrates the growth in DNSSEC zones since 2005 as measured by the SecSpider effort.

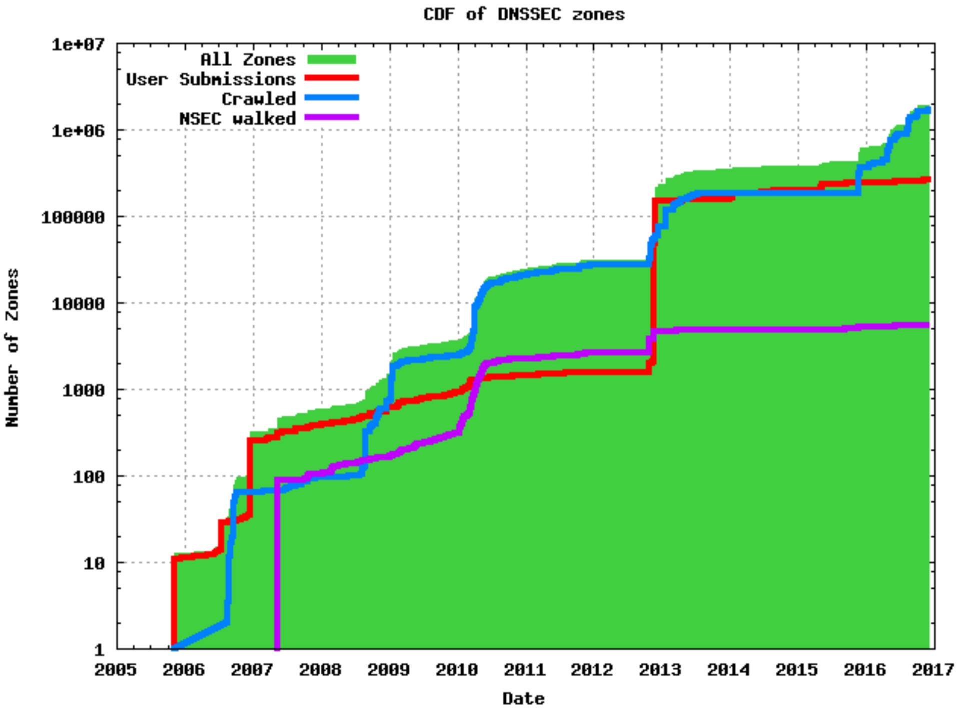

Figure 8 - SecSpider Measured Growth of DNSSEC Deployment[17]

It is useful to view the deployment of DNSSEC in .com and .net TLDs given their popularity and size as shown in Figure 9 and Figure 10.[18]

[17] http://secspider.verisignlabs.com/growth.html

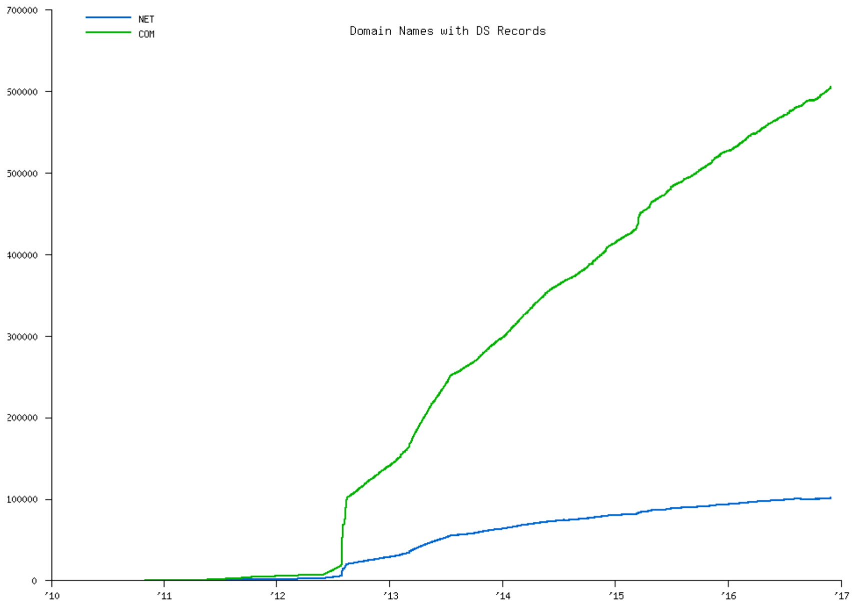

Figure 9 - Count of Domains with DS Records in .com and .net

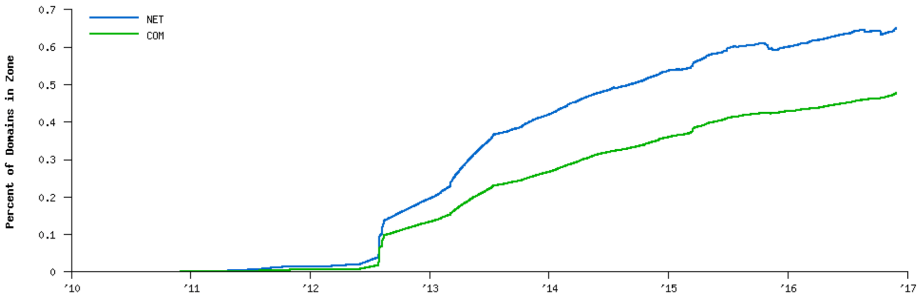

Figure 10 - Percentage of Domains with DS Records for .com and .net

NTLDstats[19] measures the deployment of new gTLDs, including deployment of DNSSEC in zones under those gTLDs. Figure 11 illustrates the growth in signed zones under the gTLDs. Although the gTLDs were required to support DNSSEC by ICANN as a condition for creation, deployment of DNSSEC in the zones under the gTLDs is voluntary by the zone owners.

[18] http://scoreboard.verisignlabs.com

[19] https://ntldstats.com/dnssec

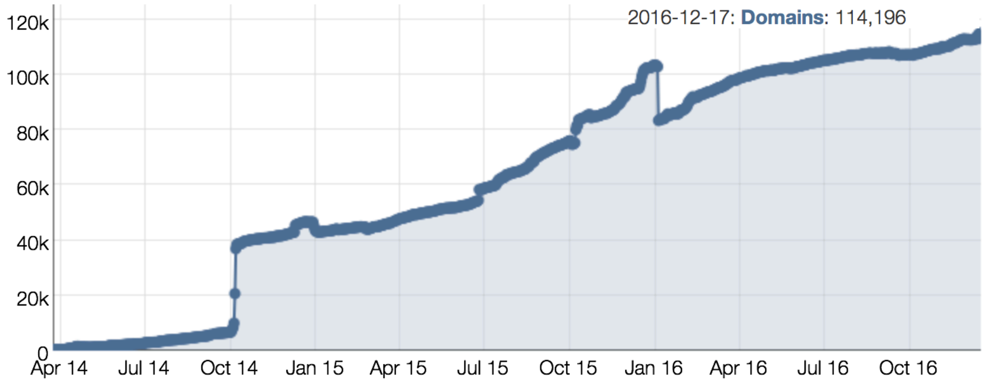

Figure 11 - Growth in signed zones in the new gTLDs[20]

At this time, NTLDstats shows that out of 26,803,748 domains, only 114,196 zones are signed (0.42%). Their numbers indicate that approximately 29% of the signed zones have DNSSEC errors. Note that NTLDstats also show that ~69% of the domains under the gTLDs are parked, though they don't break out their signed zone numbers into parked and unparked domains.

One interesting development with the new gTLDs was the requirement by two new gTLDs (.bank and .insurance) for all domains registered under those TLDs to be signed with DNSSEC. This results in 100% of those SLDs being signed. While the numbers are small right now, it will be interesting to see if this requirement catches on with any other new gTLDs.

The US Government (USG) has frequently provided the view that an appropriate role for governments to encourage deployment of new technologies in their countries by deploying the new technology in their own networks. Therefore, it is useful to look at the deployment of DNSSEC on zones within .gov. Figure 12 shows that 88% of the tested domains had enabled DNSSEC[21].

[20] https://ntldstats.com/dnssec (12/18/2016)

[21] https://fedv6-deployment.antd.nist.gov/snap-all.html (12/18/2016)

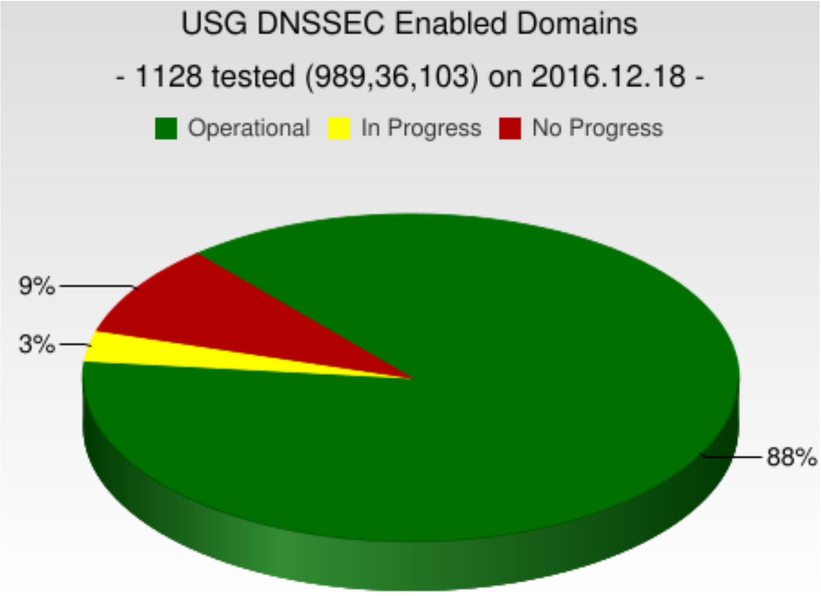

Figure 12 - Current State of USG DNSSEC enabled Domains[22]

Figure 13 illustrates the trend in enabling DNSSEC in USG domains since 2011. While this trend shows the number of domains supporting DNSSEC has levelled off or declined slightly since 2013 it also shows that the number of unsigned or domains with errors has declined.

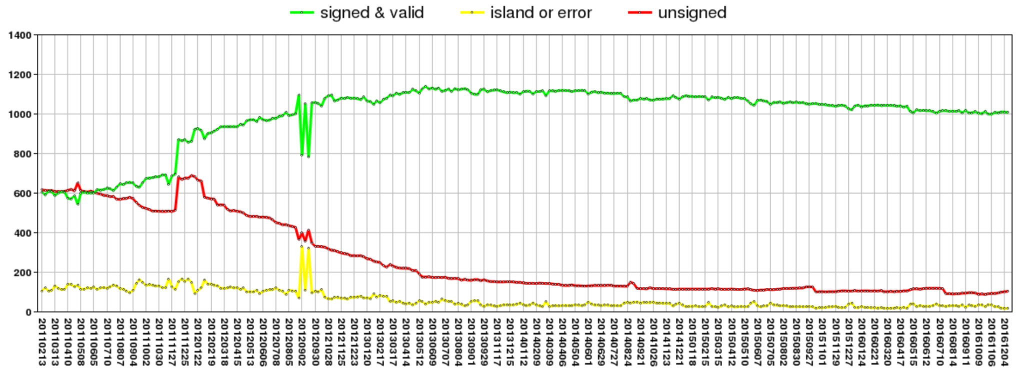

Figure 13 – Trend of USG DNSSEC Enabled Domains over Time[23]

[22] https://usgv6-deploymon.antd.nist.gov/snap-all.html (12/18/2016)

[23] https://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov (12/18/2016)

3.3 Algorithms and key sizes

DNSSEC depends on cryptographic algorithms for the following operations:

- Generating keys for signing (DNSKEY)
- DNSSEC signatures (RRSIG)
- Chain of trust (DS Record)
- Generation of NSEC/NSEC3 responses by authoritative DNS servers
- Validation of DNSSEC records by resolvers.

The security and reliability of DNSSEC depends on the algorithm and key length used. Over time, as techniques to compromise algorithms have become more sophisticated and more powerful, newer algorithms have been defined and key lengths have been increased (where applicable). Given the highly distributed nature of the DNS, new algorithms are deployed into different zones at different times as operators upgrade their systems at different rates. Table 6 provides the latest recommendations from the IETF [RFC6944], though the IETF DNS Operations (DNSOP) working group is currently developing new recommendations. [I-D.wouters-sury-dnsop-algorithm-update]. In addition, newer algorithms are being developed (e.g., [I-D.ietf-curdle-dnskey-eddsa]).

Since algorithm 6 is an alias for 3 and algorithm 7 is an alias for 5 these numbers are combined in the following tables.

Must Implement	Must Not Implement	Recommended to Implement	Optional
RSASHA1	RSAMD5	RSASHA256, RSASHA1-NSEC3-SHA1[24], RSASHA512, ECDSAP256SHA256, ECDSAP384SHA384	DSA, DH, DSA-NSEC3-SHA1[25], and ECC-GOST (Any registered algorithm not listed in this table)

Table 6 - Algorithm recommendations from RFC6944

[24] Alias for RSA/SHA1

[25] Alias for DSA/SHA1

Root Zone:

- From the first signing of the root zone (2010) until 2016, the root zone was signed using RSA/SHA-256 (8) with a Zone Signing Key length of 1024 bits.
- In September 2016, Verisign introduced 2048 bit Zone Signing Keys as part of its quarterly ZSK rollover process (not to be confused with the root KSK rollover). By the end of December 2016, this process should be complete.
- The root zone Key Signing Key is 2048 bits in length and RSA/SHA-256 is used for signing.[26]

TLD:

Table 7 illustrates the distribution of algorithms and key lengths for the TLD Key Signing Keys. The overwhelming majority (~99%) of TLDs use 2048 bit keys. ~75% of TLDs use RSA/SHA-256 for signing followed by RSA/SHA-1.

	Key Length						
Algorithm	1024b	1280b	1536b	2048b	4096b	Total	%
RSA/SHA-1	1		1	493	3	498	23.8%
RSA/SHA-256		5		1541	16	1562	74.6%
RSA/SHA-512	1			34		35	1.7%
Total	2	5	1	2068	19	2095	
%	0.1%	0.2%	0.0%	98.7%	0.9%		

Table 7 - Distribution of Algorithms & Lengths in TLD Key Signing Keys (5 December, 2016)

Table 8 illustrates the distribution of algorithms and key lengths for the TLD Zone Signing Keys. The algorithms used roughly tracks the Key Signing Keys; however, the dominant key length for the ZSKs is 1024 bits followed by 1280 bits. Since ZSKs are rolled over more frequently, the general practice is to use a shorter key length than for the KSK.

[26] https://www.iana.org/dnssec/icann-dps.txt

Algorithm	Key Length						
	1024b	1048b	1152b	1280b	2048b	Total	%
RSA/SHA-1	479			1	27	507	22.0%
RSA/SHA-256	1115	2	5	520	121	1763	76.5%
RSA/SHA-512	35					35	1.5%
Total	1629	2	5	521	148	2305	
%	70.7%	0.1%	0.2%	22.6%	6.4%		

Table 8 - Distribution of Algorithms and Lengths for Zone Signing Keys (5 December 2016)

General

As part of its SecSpider effort, Verisign Labs publishes statistics on the key signing algorithms that they see on the zones they monitor, summarized in Table 9.

Number	Algorithm	# Keys	%
1	RSA/MD5 (Deprecated)	21	0.0%
3+6	DSA/SHA-1	218	0.0%
5+7	RSA/SHA-1	1,548,639	36.4%
8	RSA/SHA256	2,453,608	57.6%
10	RSA/SHA512	13,929	0.4%
12	ECC/GOST	89	0.0%
13	ECDSA Curve P-256 with SHA-256	211,078	5.6%
14	ECDSA Curve P-384 with SHA-384	484	0.0%

Table 9 - SecSpider Distribution of key algorithms (23 December 2016)[27]

Similar to the TLD numbers[28], RSA/SHA256 is the algorithm used in the majority of zones followed by RSA/SHA-1. Elliptic Curve Digital Signature Algorithm (ECDSA) is the newest algorithm defined for DNSSEC and is used in ~5% of zones monitored (note that none of the TLDs use ECDSA). SecSpider doesn't break out KSKs and ZSKs and doesn't provide the key lengths used.

[27] http://secspider.verisignlabs.com/stats.html

[28] Snapshot on 12/6/2016 from http://secspider.verisignlabs.com/stats.html (numbers updated daily)

4 State of Deployment of DNS-based Authentication of Named Entities (DANE)

The requirements for DNS-Based Authentication of Named Entities (DANE) were published in 2011 [RFC6394] with TLSA records defined in 2012 [RFC6698] and operational guidance in 2015 [RFC7671]. DANE defines a way "to use the DNSSEC infrastructure to store and sign keys and certificates that are used by TLS" as well as binding public key data to DNS names. While DANE deployment has been slow, it has picked up recent support, especially in securing transfers between email servers [RFC7672]. This recent growth is reflected in the recent growth in number of zones deploying TLSA as measured by Verisign Labs (see Figure 14).

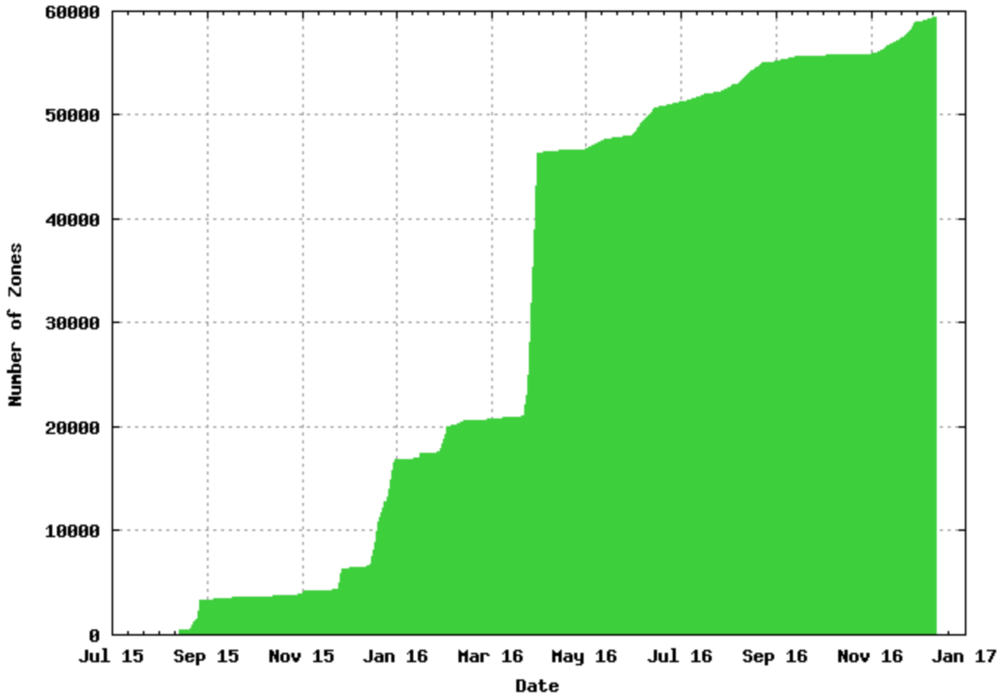

Figure 14 - TLSA Deployment[29]

[29] http://secspider.verisignlabs.com/pix/tlsa-growth.png (12/18/2016)

Verisign Labs also provides a breakdown of the services for which there is a TLSA record:

Number of Zones	Service (Port number)
732	Secure SMTP (Port 465)
235	Secure POP3 (Port 995)
897	SMTP with STARTTLS (Port 587)
63	Alternate SMTP (Port 2525)
5,980	HTTPS (Port 443)
3,931	SMTP (Port 25)
129	POP3 (Port 110)
528	Secure IMAP (Port 993)
348	IMAP (Port 143)

Table 10 - Services with TLSA Records[30]

DANE (similar to DNSSEC) requires support from DNS Servers to hold the TLSA records and clients (including resolvers) to utilize the TLSA records.

DNS Servers supporting DANE (TLSA records) include[31]:

- BIND (from version 9.9.x)
- NSD (from version 3.2.11)
- PowerDNS (from version 3.0)
- Microsoft DNS (from Windows Server 2016)
- Knot DNS (from version 1.0.4)
- YADIFA (from version 2)

[30] http://secspider.verisignlabs.com/stats.html (12/18/2016)

[31] https://bsidesljubljana.si/wp-content/uploads/2016/03/P-DANE.pdf

Mail servers supporting DANE include:

- Postfix support since 2014 (3.1 or later recommended)
- Halon support since 2015
- Exim 4.85 (experimental)
- Sendmail - no support (patch available[32])
- Exchange Server - no support (3rd party solution: XWall/CryptoFilter[33])

Web browsers: No major web browser supports DANE, though cz.nic has developed a DNSSEC/TLSA Validator browser add-in.

Libraries:

- OpenSSL (DANE from 1.1.0) (ECDSA from 0.9.8)
- gnutls (from 3.1.3)

Over the past few years, DANE deployment has picked up steam securing transport of email between servers, driven by German email providers. DANE alleviates one of the major burdens of running TLS between servers by making it easier to acquire the keys for a remote server as needed and allows a mail provider to signal the enforcement of TLS use (preventing downgrade-STARTTLS attacks). In May, 2016 two of the largest email providers in Germany (web.de and GMX) enabled support for DANE as part of the "Email made in Germany" effort[34]. These two providers represent over 50% of the German email market.

[32] http://www.five-ten-sg.com/util/sendmail-8.16.0-dane.patch

[33] http://www.dataenter.com/doc/cryptofilter.htm

[34] https://de.wikipedia.org/wiki/E-Mail_made_in_Germany

Victor Dukhovni has been tracking domains with TLSA records for MX hosts and has found that the number exceeds 103,000 as of 4 December 2016. He has also found that the hosting providers with the top 5 counts of DANE SMTP domains are:

# DANE SMTP Domains	Hosting Providers
42,140	domeneshop.no
32,656	transip.nl
15,097	udmedia.de
1,758	bhosted.nl
1,273	nederhost.net

Table 11 - Top 5 Hosting Providers with DANE SMTP domains[35]

National governments have started including use of DANE to secure email in their requirements and recommendations. In September 2016, the National Institute of Standards and Technology (NIST) published Special Publication 800-177 [SP800177] on trustworthy email that includes DANE as one of its methods[36]. In May 2016, Germany's Bundesamt für Sicherheit published TR-03108 containing its technical guidelines for secure email transport[37]. The Netherlands also added DANE (with STARTTLS) to its "use or explain" list.[38][39]

Work is underway in both the IETF and in the field to further define usage of DNSSEC to secure email, e.g., SMIMEA [SP1800-6][SMIMEA] and OPENPGPKEY [RFC7929].

[35] email from Viktor Dukhovni to the dane@ietf.org mail list on 12/4/2016

[36] https://www.nist.gov/node/1099976

[37] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03108/index_htm.html

[38] https://www.forumstandaardisatie.nl/standaard/starttls-en-dane

[39] https://www.sidnlabs.nl/a/weblog/new-e-mail-security-protocols-mandatory-within-government?language_id=2&langcheck=true

5 Root Key Signing Key (KSK) Rollover

While the root ZSK rollover is a regularly scheduled quarterly event, ICANN's practice for the root KSK rollover is every 5 years, or as required.[40] Due to its potential for disruption, KSK Rollover plans are carefully developed by Root Zone Management Partners:

- ICANN (as IANA Functions Operator)
- Verisign (as Root Zone Maintainer)
- NTIA (as Root Zone Administrator. Note that this role ended as of 1 October 2016.)

The first-ever root KSK rollover process began on October 27, 2016 when ICANN generated the new KSK[41]. The rollover process will continue through 2018, when the old KSK and backups should be deleted from all systems. The draft timeline for the remaining steps in the rollover are:

- **February 2017**: New KSK published in Trust Anchor XML file at http://data.iana.org/root-anchors/
- **July 2017:** New KSK published in root zone as part of DNSKEY RRset signed by the old KSK.
- **September 2017:** Size increase for DNSKEY response from root name servers.
  - Root name servers include both old and new KSK DNSKEY in responses
- **October 2017:** Begin signing the root zone DNSKEY RRset with new KSK (Actual rollover event).
- **January 2018:** Old KSK is published in root zone DNSKEY RRset with revoked bit set. DNSKEY RRset includes new KSK.
- **March 2018:** Remove old KSK from the root zone.
- **May/August 2018:** Old KSK and all backups deleted

[40] ICANN, "DNSSEC Practice Statement for the Root Zone KSK Operator," 1 October, 2016, https://www.iana.org/dnssec/dps/ksk-operator/ksk-dps.txt

[41] https://www.icann.org/news/blog/ksk-rollover-operations-begin

The new KSK will maintain the same algorithm (RSA/SHA-256) and key length (2048 bits) as the previous KSK. For more information, see ICANN's Root Zone KSK Rollover web site[42].

6 Challenges to Deployment

In the signing of the root zone in 2010, one of the largest impediments to deployment of DNSSEC was removed, providing a chain of trust to the root. During this time, the DNSSEC Deployment Initiative[43] was active in promoting the deployment of DNSSEC. In 2012, ISOC published a white paper examining the challenges to deployment of DNSSEC on the Internet.[44] The Internet Society instituted their Deploy360 Programme providing information, tutorials and other resources to help with the deployment of DNSSEC[45]. The DNSSEC Deployment Initiative, the ISOC Deploy360 Programme and ICANN's Security and Stability Advisory Committee (SSAC) continue to jointly organize a full day workshop on DNSSEC deployment at ICANN meetings.

Great strides have been made since 2012 in addressing the challenges identified, as can be seen by the growth in number of TLDs signed, general availability of validating resolvers and wider availability of tools; however, many of the challenges still need to be addressed, such as availability of DNSSEC-aware applications.

6.1 Challenges with changing cryptographic algorithms

As attacks on cryptography improve and as research into new cryptographic (often simply called "crypto") algorithms progresses, new crypto algorithms will need to be deployed in DNS. As can be seen in Section 4.3, different crypto algorithms and key lengths are deployed in different zones and can be supported in the Internet at present (e.g., .com uses RSA/SHA-256 and cloudflare.com uses ECDSA Curve P-256). The

[42] https://www.icann.org/resources/pages/ksk-rollover

[43] https://www.dnssec-deployment.org/

[44] http://www.internetsociety.org/deploy360/resources/whitepaper-challenges-and-opportunities-in-deploying-dnssec/

[45] http://www.internetsociety.org/deploy360/dnssec/

challenge occurs when a zone is migrated from one crypto algorithm to another. The impact of the migration will generally depend on how large the zone is and the criticality of operation of the sub-zones.

An Internet-Draft under development [CRYPTOALG] discusses the challenges in deploying new crypto algorithms. This I-D identifies challenges in the following areas when deploying new algorithms.

- DNS resolvers performing validation
    - New algorithms will generally require updating resolver software
    - New algorithms could trigger undetected bugs and non-updated software must handle unknown algorithms correctly.
    - Potential increased CPU load and memory requirements.
    - See [RFC8027] for more information on problems validators might see with noncompliant infrastructure.
- Authoritative DNS servers
    - Zone updates need to be capable of using new algorithms in creation of NSEC or NSEC3 records in the zone.
    - Servers that use some form of dynamic response to provide NSEC or NSEC3 records need to incorporate new algorithms into their response function.
- Signing software (including user interfaces)
    - Update needed to support the new algorithm.
    - Update might be needed to support rollover.
- Registries
    - Registries must be able to support the codepoint for the new algorithm in DS Records for lower level zones, even if the registry doesn't use the new algorithm.
- Registrars
    - Software and systems must be able to support new algorithm codepoints in its verification process for creation of DS Records.
    - Communication with registries and DNS hosting operators may need to be updated to support the new algorithm.

- DNS Hosting Operators
    - Must update authoritative DNS servers and associated provisioning software to support the new algorithm
    - A new algorithm could also affect the CPU load and memory requirements.
- Applications
    - Applications that perform DNSSEC validation would need to be updated to support the new algorithm.

6.2 Case study - Elliptic Curve Digital Signature Algorithm (ECDSA) rollout

An example of the migration to a new crypto algorithm is the deployment of the Elliptical Curve Digital Signature Algorithm [RFC6605] published in 2012. This algorithm is reported to provide shorter key lengths while providing the same level of cryptographic protection as longer keys used by RSA.[EDCSAIMP] While Unbound and BIND have supported ECDSA for several years it can take time to integrate the new software release into products. There can also be delays in turning on the new capability in the field. Discussions have also indicated that at least one registrar did not support ECDSA simply because the user interface in their provisioning systems didn't allow the algorithm to be selected.

Studies done by APNIC Labs illustrate the support of ECDSA P-256 in validating resolvers, see Figure 15 and Table 12[46]. These studies indicate that, except for a few countries, support for ECDSA in resolvers is roughly equivalent (slightly less) to support for RSA.

The SecSpider results summarized in Table 9 indicate that approximately 5% of zones studied are signed by ECDSA. While the majority of this usage can be attributed to Cloudflare's support for ECDSA, [ECDSACASE] indicates that other DNS providers are starting to support ECDSA. [ECDSACASE] provides a good case study of the deployment of ECDSA and some of the difficulties it faces.

[46] http://stats.labs.apnic.net/ecdsa?s=ECDSA

While an advantage given for migrating to ECDSA is the reduction in the size of signatures (compared to RSA) with a resulting reduction in fragmentation of responses and reduction of potential amplification factor, one of the concerns expressed about the use of ECDSA is the increased CPU load in resolvers. A recent study by researchers at the University of Twente indicate that, while ECDSA validation does increase the load on resolvers as compared to RSA, it does not do so beyond the capacity of modern CPU cores. The study addresses a potential denial of service attack on a resolver due to CPU attack and suggests a countermeasure utilizing rate-limiting in resolvers. [ECCRESOLVE]

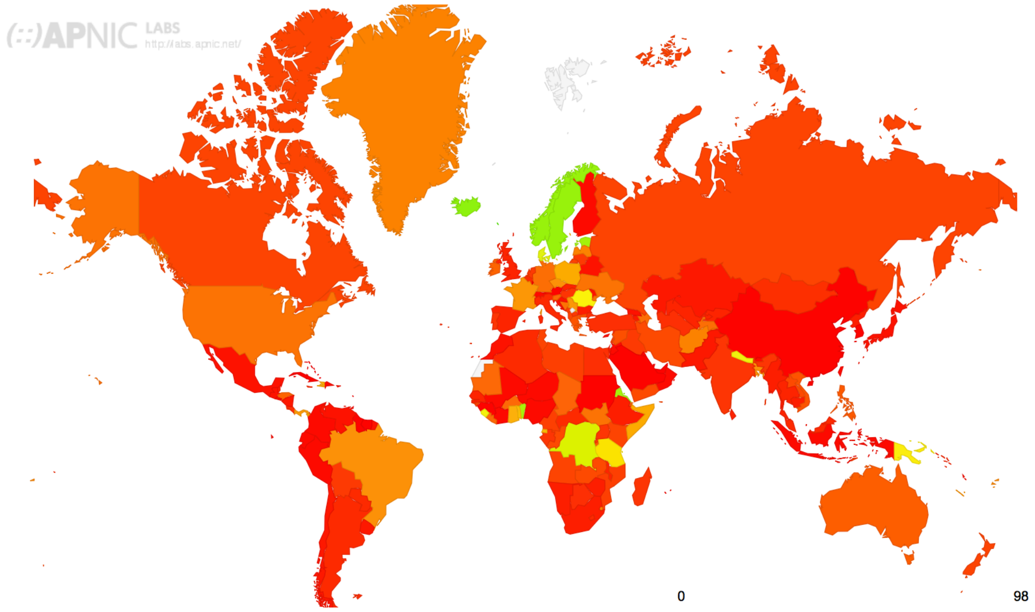

Figure 15 - APNIC DNSSEC ECDSA Validation Rate by country (%)

Region	ECDSA Validates	RSA Validates	ECDSA and RSA Validates	Uses Google PDNS
World	11.69%	14.78%	10.82%	14.44%
Unclassified	44.48%	48.95%	41.82%	37.04%
Americas	19.44%	22.27%	19.02%	12.94%
Oceania	17.96%	23.65%	17.77%	5.50%
Europe	17.79%	19.68%	16.44%	9.42%
Africa	10.73%	16.22%	8.71%	29.99%
Asia	7.11%	10.14%	6.47%	13.52%

Table 12 - Resolver Support for ECDSA by Region

6.3 Automation of secure delegations

Another DNSSEC deployment challenge that received significant attention during 2016 was the area of automating the updates of DNS records related to the global "chain of trust" used in validation.

To create a chain of trust from the root of DNS down to a second level domain, Delegation Signer (DS) resource records [RFC3658] are used to connect the child zone to the parent zone (typically, but not always, a TLD). The registry operating the parent zone requires that the operator of the child zone upload a DS record (or in a few cases a DNSKEY record) through typically a web interface or some form of application programming interface (API).

The challenge is that the current operation model requires that the registrar for a given domain name be the one to provide the update to the registry. This works fine if the registrar is also the operator of the authoritative DNS servers for the domain. However, if the domain registrant is using a different entity to operate the authoritative DNS servers, or are operating their own authoritative DNS servers, the registrar must still be involved. Given that current best practices for DNSSEC involve annually rolling the KSK, this requires at least an annual update of the DS or DNSKEY records via the registrar.

Unfortunately this is not easily automated, given the wide range of different systems used by registrars and registries. [RFC7344] offered one approach and a new Internet draft in 2016, [I-D.ietf-dnsop-maintain-ds], provided updates to improve this process.

Another proposal has been submitted to the IETF Registry Extensions (REGEXT) working group, [I-D.ietf-regext-dnsoperator-to-rrr-protocol][47] and active implementations are underway by both CIRA[48] and Gandi[49]. Signers such as CloudFlare and Gandi are working with registries behind TLDs including .CA (Canada) and .CL (Chile) to test these implementations.

[47] https://tools.ietf.org/html/draft-ietf-regext-dnsoperator-to-rrr-protocol-01

[48] https://github.com/CIRALabs/DSAP/

[49] https://github.com/kalou/rrr

7 Conclusion

Since the DNS root zone was signed in 2010, the deployment of DNSSEC has made steady progress. Almost all of the gTLDs are now signed and approximately half of the ccTLDs, including over 90% of the ccTLDs from OECD countries. Progress among Second Level Domains has been slower globally, but with areas of greater deployment depending on the TLD and region (e.g., .nl, .cz, .se, .gov). Most major authoritative server software now supports DNSSEC with increasingly better tools for managing deployment and operation.

On the resolver side, all the major resolver software supports DNSSEC validation. APNIC's studies have shown that resolvers used by over 80% of clients in their study already query for DNSSEC records even if they haven't currently enabled validation. As illustrated by Claro and Comcast, a single large provider turning on validation for its customers can substantially change the complexion of validation in in a country.

An example of a service driving deployment in a particular community is the use of DANE to secure email between servers. The German email community has taken the lead in utilizing DANE to secure communication between email providers and support is spreading to other European providers.

Development continues to evolve as DNSSEC is more widely deployed and gains more operational experience and as DNS-based attacks continue to be a concern (e.g., amplification attacks, DNSChanger). As an example, ECDSA has been proposed as a way to reduce amplification attacks and using DNSSEC's built-in functionality to identify non-existent domains via NSEC records to terminate certain attack traffic at the resolver.[AGGNSEC] In addition, work is ongoing to protect the link between the client and the validating resolver.

We encourage all readers of this report to, at a minimum, deploy DNSSEC validation to begin checking signatures and then to understand their options for signing their domains. Together we can create a stronger and more trusted DNS.

8 References

[ECCRESOLVE] van Rijswijk-Deij, R., Hageman, K., Sperotto, A., and A. Pras, "The Performance Impact of Elliptic Curve Cryptography on DNSSEC Validation," in *IEEE/ACM Transactions on Networking* , vol.PP, no.99, pp.1-13, 22 September 2016.

[ECDSACASE] van Rijswijk-Deij, R., Sperotto, A., and A. Pras, “Making the Case for Elliptic Curves in DNSSEC.” in ACM SIGCOMM Computer Communication Review 45(5):13-19 · September 2015

[KAMINSKYBUG] Wright, Cory, “Understanding Kaminsky's DNS Bug,” Linux Journal, July 2008 (http://www.linuxjournal.com/content/understanding-kaminskys-dns-bug)

[RFC2065] Eastlake 3rd, D. and C. Kaufman, "Domain Name System Security Extensions", RFC 2065, January 1997.

[RFC3658] Gudmundsson, O., "Delegation Signer (DS) Resource Record (RR)", RFC 3658, December 2003.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC6394] Barnes, R., "Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)", RFC 6394, October 2011.

[RFC6605] Hoffman, P. and W. Wijngaards, "Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC", RFC 6605, April 2012.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

[RFC6944] Rose, S., "Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status", RFC 6944, April 2013.

[RFC6891] Damas, J. and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))," RFC 6891, April 2013.

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

[RFC7671] Dukhovni, V. and W. Hardaker, "The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance,' RFC 7671, October 2015.

[RFC7672] Dukhovni, V. and W. Hardaker, "SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)," RFC 7672, Oct. 2015.

[RFC7929] P. Wouters, "DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP," RFC 7929, August 2016.

[APNICM] Geoff Huston, "Measuring DNSSEC Performance", APNIC Labs, 30 Apr 2013, (https://labs.apnic.net/?p=341).

[CRYPTOALG] York, D. , Sury, O., Wouters, P. and O. Gudmundsson, "Observations on Deploying New DNSSEC Cryptographic Algorithms," draft-york-dnsop-deploying-dnssec-crypto-algs-04, November, 2016. (work in progress)

[SP800177] National Institute of Standards and Technology Special Publication 800-177, "Trustworthy Email," September 2016.

[SP1800-6] National Institute of Standards and Technology Special Publication 1800-6, "Domain Name Systems-Based Electronic Mail Security", November 2016, (DRAFT).

[SMIMEA] Hoffman, P and J. Schlyter, "Using Secure DNS to Associate Certificates with Domain Names For S/MIME," draft-ietf-dane-smime-14, November 2016, work in progress.

[ECDSAIMP] Khalique, A., Singh, K., and S. Sood, "Implementation of Elliptic Curve Digital Signature Algorithm", May 2010. (Web. http://www.ijcaonline.org/volume2/number2/pxc387876.pdf)

[I-D.wouters-sury-dnsop-algorithm-update] Wouters, P. and O. Sury, "Algorithm Implementation Requirements and Usage Guidance for DNSSEC," draft-wouters-sury-dnsop-algorithm-update-02 (work in progress), October 2016.

[I-D.ietf-curdle-dnskey-eddsa] Sury, O. and R. Edmonds, "EdDSA for DNSSEC", draft-ietf-curdle-dnskey-eddsa-01 (work in progress), October 2016.

[I-D.ietf-dnsop-maintain-ds] Gudmundsson, O., and P. Wouters, "Managing DS records from parent via CDS/CDNSKEY", draft-ietf-dnsop-maintain-ds-04, October 2016.

[I-D.ietf-regext-dnsoperator-to-rrr-protocol] Latour, J., Gudmundsson, O., Wouters, P., and M. Pounsett, "Third Party DNS operator to Registrars/Registries Protocol", draft-ietf-regext-dnsoperator-to-rrr-protocol (work in progress), July 2016

[AGGNSEC] Fujiwara, K., Kato, A. and W. Kumari, "Aggressive use of NSEC/NSEC3," draft-ietf-dnsop-nsec-aggressiveuse-03, October 2016, work in progress.

9 Appendix: Resources

Deploy360 DNSSEC Programme:

- https://www.internetsociety.org/deploy360/

DNSSEC Deployment Initiative:

- http://www.dnssec-deployment.org

ICANN DNSSEC Resources

- https://www.icann.org/resources/pages/dnssec-2012-02-25-en

10 Acknowledgements

This 2016 report was prepared by Chip Sharp with input from Dan York. We appreciate the proofreading and feedback of the following people: Steve Crocker, Paul Ebersman, Geoff Huston, Fabhia Kumari, Megan Kruse, Rick Lamb, Jacques Latour, Hugo Salgado-Hernández and Paul Wouters.

We thank all of the members of the DNSSEC community who share their data and are working each day to raise the level of trust in the DNS.

Please send any feedback on this report to Dan York at york@isoc.org.