SSAC DNSSEC Operational Considerations Work Party: Introduction and Updates

WP Co-chairs: Chaoyi Lu, Ram Mohan

June 2025

https://chaoyi.lu

WP Overview

DNSSEC Operational Considerations

WP co-chairs	Chaoyi Lu and Ram Mohan
Contributors	Steve Crocker, James Galvin, Geoff Huston, Warren Kumari, John Levine, Russ Mundy, Peter Thomassen, Rick Wilhelm
Reviewers	Joe Abley, Rod Rasmussen
Observers	Tim April
Invited guests (tentative)	Mark Elkins, Eric Osterweil

WP Timeline

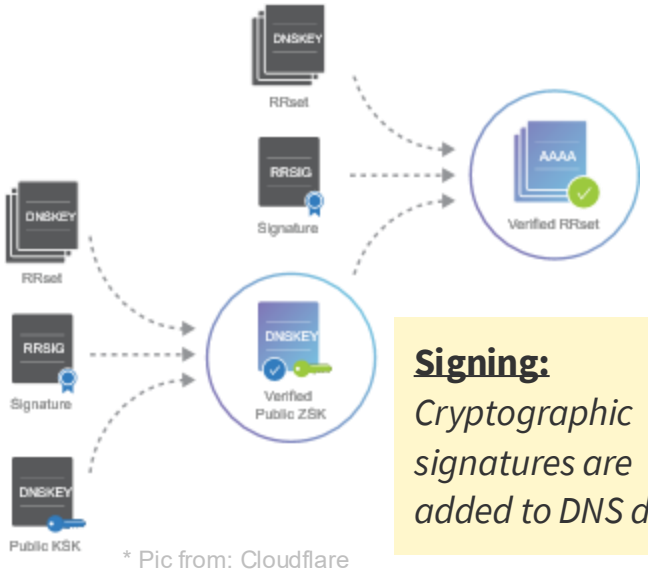
- **Sept 2024: DNSSEC Assessment Work Party *(terminated)***
  - **Goal:** Assess **current state** of DNSSEC deployment; determine what **value** DNSSEC provides to opperators and users of the Internet

---

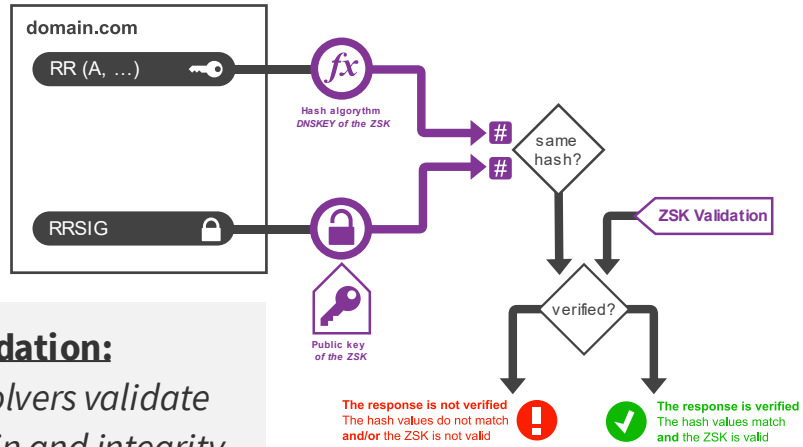
- **Mar 2025: ICANN82 Seattle**
  - Ideas of reviving a DNSSEC WP, about its current state and operational considerations
- **Apr 2025: WP kick-off meeting**
- **May 2025: WP Charter finalized**
  - **Goal:** Understanding the **practical realities** of deploying and operating DNSSEC, summarizing current state and determinants of deployment.
- **Jun 2025: Developing report outline *(where we are now)***

WP Charter - Motivation (1)

- **Plain-text DNS resolutions are susceptible to manipulation**
  - Cache poisoning, MITM hijacking, path incerception, etc
- **DNSSEC ensures origin and data integrity by signing and validation**



Signing:
Cryptographic signatures are added to DNS data



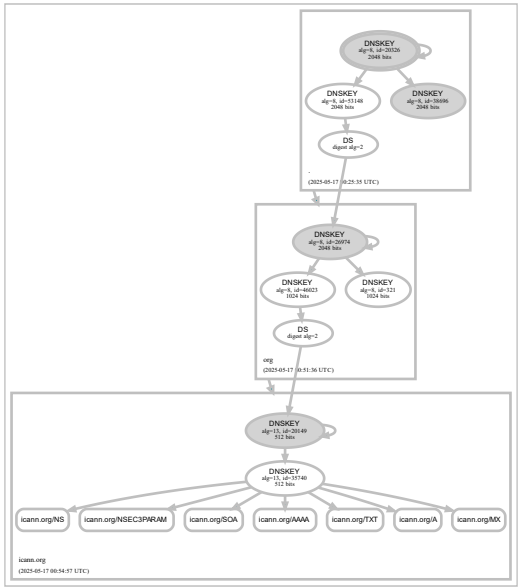
Validation:
Resolvers validate origin and integrity of DNS data

* Pic from: Cloudflare

* Pic from: EfficientIP

WP Charter - Motivation (2)

- **Operational challenges have arisen at stages of deployment**



Building chain of trust

VERISIGN // BLOG

HOME

THE 2024-2026 ROOT ZONE KSK ROLLOVER: INITIAL OBSERVATIONS AND EARLY TRENDS

MARCH 19, 2025 • BY DUANE WESSELS • SECURITY

Rolling the algorithm

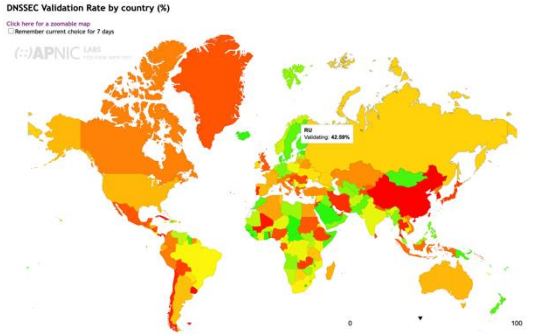
All Verisign TLDs are currently signed with DNSSEC algorithm 8, also known as RSA/SHA-256, as documented in our DNSSEC Practice Statements. Currently, we use a 2048-bit Key Signing Key (KSK), and 1280-bit Zone Signing Keys (ZSK). The RSA algorithm has served us (and the broader Internet) well for many years, but we wanted to take the opportunity to implement more robust security measures while also making more efficient use of resources that support DNSSEC-signed domain names.

We are planning to transition to the Elliptic Curve Digital Signature Algorithm (ECDSA), specifically Curve P-256 with SHA-256, or algorithm number 13, which allows for smaller signatures and improved cryptographic strength. This smaller signature size has a secondary benefit, as well: any potential DDoS attacks will have less amplification as a result of the smaller signatures. This could help protect victims from bad actors and cybercriminals.

Keys and rollover

Analyzing DNSSEC problems for icann.org

.	Found 3 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
org	Found 1 DS records for org in the . zone DS=26974/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=53148 and DNSKEY=53148 verifies the DS RRset Found 3 DNSKEY records for org

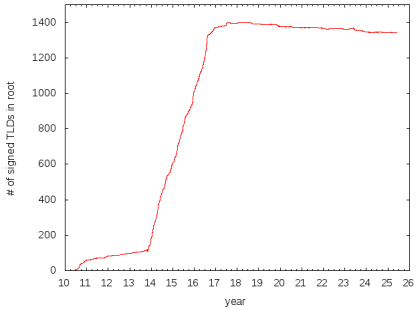


Tooling and monitoring

WP Charter - Motivation (3)

- **Deployment status 15+ years in**

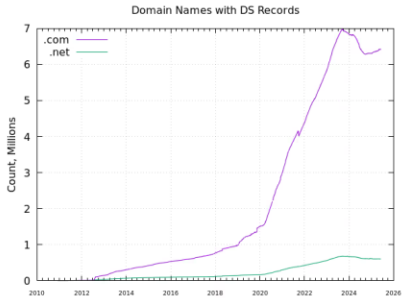
Signing rates



TLDs:

>1,340 (93%) *have been signed*

Source: Rick Lamb
http://rick.eng.br/dnssecstat/

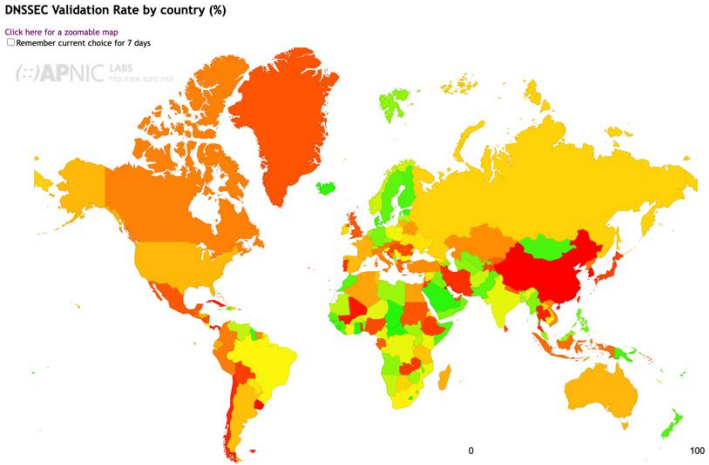


SLDs:

~7% *have been signed*

Most top sites also remain unsigned

Validation rates



World-wide: ~35% users are validating

Source: APNIC (https://stats.labs.apnic.net/dnssec)

WP Charter - Motivation (4)

- **Some DNSSEC incidents or outages**

DNSSEC chain validation issue for .nz

Incident Report for InternetNZ

Postmortem Following the DNSSEC chain validation issue for .nz domains on 29-31 May 2023, we have now published the independent review on the InternetNZ website..

.com.au RRSIG Expired

Matt Corallo nanog at as397444.net
Mon Sep 18 00:48:11 UTC 2023

- Previous message (by thread): Canadian regulator CRTC hires private company to investigate 2022 Rogers outage
- Next message (by thread): *.au RRSIG Expired
- **Messages sorted by:** [date] [thread] [subject] [author]

Just in case anyone wonders why *.com.au isn't loading for their customers, the RRSIG covering .com.au/DS expired at 00:05:29 UTC (about 40 minutes ago now).

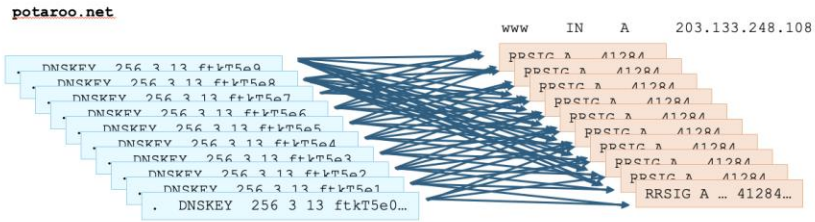
Matt

KeyTrap

By Geoff Huston on 12 Mar 2024

Category: Tech matters

Tags: DNS, DNSSEC, security



WP Charter – Scope (1)

Overview	Describe DNSSEC's purpose, mechanisms, and intended benefits
Current state analysis	• Deployment status investigated by **literature, reports, and studies** • Interaction of **DNSSEC and security** • **Current level of deployment** across different parts of the DNS ecosystem • **Longitudinal changes** over time
Determinants of DNSSEC deployment	• Identify the **technical and operational factors** that influence the decision to deploy (or not deploy) DNSSEC. • Investigate **why certain factors act as facilitators or barriers** to DNSSEC • Where possible, list potential mitigation strategies to identified barriers
Data collection	• Potential **survey** of DNS operators to gather information on DNSSEC experiences • Potential follow-up **interviews** to gather more in-depth qualitative data • Analysis of publicly available **data**

WP Charter – Scope (2)

- **Out of scope:**
  - Evaluating the **fundamental value** of DNSSEC: This work party will operate under the baseline assumption that DNSSEC, in its current form, is the established standard for securing DNS data. The focus will be on its implementation.
  - Consideration of **financial costs, market analysis, or business cases** related to DNSSEC deployment.

WP Charter – Target Audience & Timeline

- **Target Audience:**
  - Primary: DNS operators, registries, and registrars
  - Secondary: ICANN Board, specification authors, software implementers, and the DNS security community

- **Timeline (tentative):**
  - **Development of initial draft (work party)** June 9 - Aug 25 [6-10 weeks]
  - **SSAC full review (work party, SSAC)** Sep 1 - Sep 28 [4 weeks]
  - **Development of final draft, iterate additional reviews on new text as needed (work party, SSAC)** Oct 6 - Nov 17 [5-6 weeks]
  - **Finalization (SSAC, staff, Board)** - Early 2026
  - **Publication & dissemination - ICANN 85 Mumbai** (7-12 March 2026)

SSAC DNSSEC Operational Considerations Work Party

WP Co-chairs: Ram Mohan, Chaoyi Lu

June 2025

https://chaoyi.lu