Root Zone Algorithm Rollover

How to change to DNSSEC algorithm signing the root zone

James Mitchell & Jakob Schlyter

IIANA Community Day, Brussels
17 November 2022

ICANN

Agenda

This presentation is about the process of changing the algorithm for signing the root zone.

- Background
- About the design team
- Design team tasks
- Next steps

What is an Algorithm Rollover?

- **DNSSEC Zone Signing Keys** (ZSK) are changed periodically – for the root zone ever 3 months. Changing the ZSK has no impact on trust anchor management.
- **DNSSEC Key Signing Keys** (KSK) are changed less frequently – for the root zone about every 5 years. The lask KSK rollover was executed in 2018. Changing the root zone KSK has impact of trust anchor management.
- The **algorithm used for signing** (currently RSA/SHA-256) has never been changed. This talk is about changing this algorithm.
- Changing the signature algorithm includes **changing both the KSK and the ZSK**.

Algorithm Rollover Design Team

ICANN plans to convene a design team of experts who will help define the steps and timelines needed to realize the algorithm rollover.

The team will develop a framework to help prepare the ICANN community and ICANN's global partners to be technically and operationally prepared for a future change in the signing algorithm.

Composed of staff, root zone management partners, and experts from the community.

The design team will build upon the experience from the *Root Zone KSK Rollover Plan* from 2016. More information on KSK rollovers are available at https://www.icann.org/resources/pages/ksk-rollover.

Design Team Experts

The design team will have experts with one or more of the following skills:

- Experience with DNSSEC algorithm rollovers, particularly in top-level domains.
- Experience in applied cryptography, particularly in the digital signature methods used in DNSSEC.
- Experience in actively participating or leading groups that designate new cryptographic algorithms for public use.
- Experience in DNSSEC software development for authoritative servers, validating resolvers, or both.

Design Team Tasks

1. How to execute an algorithm roll?
2. Criteria for selecting the algorithm
3. Deployment considerations

Algorithm Rollover

- Operational considerations
- Protocol considerations
  - RFC 5011 rollover
  - Distribution of the trust anchor
  - Requirements to sign with all algorithms
- Impact on Root Zone KSK and ZSK Management
  - Coordination of KSK and ZSK rollover
  - Dependencies on existing tools & equipment
- Cryptographic considerations
- Coordination and communication

Algorithm Rollover

- Impact on validating resolvers
  - Packet size considerations
  - DNSSEC validation behaviour
- Testing
- Implementation
- Rollback
- Schedule
  - Interplay with existing KSK and ZSK rollover processes
- Risk analysis

Algorithm Selection Criteria

The design team will develop a selection criteria for selecting the algorithm.

- Standardization status
  - Is the proposed algorithm standardized and well defined?
- Implementation support
  - Is the proposed algorithm widely supported by components used for signing and validation?
- Deployment considerations
  - Is the proposed algorithm widely deployed among validating resolvers?
  - What's on the wire during the algorithm roll?

Algorithm Candidates

The following currently defined algorithms are the most likely possible candidates for a new root key algorithm, should we roll in the near future:

- Elliptic Curve Digital Signature Algorithms (RFC 6605)
  - Curve P-256 with SHA-256 (13)
  - Curve P-384 with SHA-384 (14)
- Edwards-Curve Digital Security Algorithms (RFC 8080)
  - Ed25519 (15)
  - Ed448 (16)

Timeline

November 2022	Call for volunteers
January 2023	Design team members presented and work begins
March 2023	Presentation and dialogue at IETF 116 in Yokohama
May 2023	Draft report for public comment
June 2023	Final report

More information?

If you are interested in joining the design team, please apply before November 25, 2022, via the ICANN website.

More information available at:

- https://www.icann.org/resources/pages/ksk-algorithm-rollover-en

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg