Root Zone Algorithm Rollover

How to change to DNSSEC algorithm signing the root zone

James Mitchell et al.

IETF 116, Yokohama
29 March 2023

Agenda

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

- Background
- About the design team
- Design team tasks and thoughts
- Related and future work
- Questions

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 has convened 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.

Design Team

- James Mitchell
- Roy Arends
- Jakob Schlyter
- Paul Hoffman
- Matt Larson
- Ed Lewis
- Andres Paves
- Aaron Foley
- Duane Wessels
- Ramana Lavu
- Howard Eland
- Moritz Muller
- Peter Thomassen
- Ralf Weber
- Scott Rose
- Tomofumi Okubo
- Yoshiro Yoneya

Design Team Tasks

- How to implement and execute an algorithm rollover
- Testing the proposed implementation
- How to select an algorithm

The design team will **not decide if and when** the algorithm should be changed.

Impact

- Home devices and other middleboxes
- Stub resolvers – minimal since stub DNSSEC validation is rare.
- Validating recursive resolvers – lose benefits of DNSSEC if new algorithm not supported.
- All recursive resolvers – may experience an increase in response sizes and/or queries over TCP due to DO bit.
- Root server operators –
  - larger root zone file
  - larger responses, more TCP
  - possibly increased query load from misbehaving resolvers
- IANA/RZM – more complex key signing ceremonies, zone publication, and signature management

DNS Protocol Clarifications

Review of relevant RFC documents indicates clarifications are in order:

- Documents do not adequately address changing algorithms
- Delegation Signer (DS) resource records and trust anchors are similar but are not the same
- Some rules have led to bugs and difficulties in operational procedures

Anticipated clarifications include:

- Validators must be optimistic; any path from a Trust Anchor must be accepted by a validator
- Any valid trust chain is necessary and sufficient
- Signers need not include signatures for all algorithms, and further details

DNS Message Size Considerations

- Since the DNS flag day 2020, many root servers limit UDP packet size to 1232 bytes resulting in truncation and requery over TCP for larger response packets.
- The design team is currently working under the assumption that root server operators and validating resolvers will be able to handle the increased TCP traffic resulting from larger responses during a rollover.
  - N.B. Validating resolvers on the Internet today already have to handle large messages as many ccTLD/gTLD use large and/or multiple keys.
- DNS Message Size considered in algorithm selection criteria

Algorithm Selection Criteria

How to select an algorithm:

- Protocol Considerations
- Implementation / Deployment / Availability Considerations
  - Standardization and implementation requirements
- Cryptographic
- Operations Considerations
- Impact on Root Zone KSK/ZSK Management
- Impact on Validating Resolvers
- DNS Message Size Considerations
- DNSSEC Validation Behaviour

Algorithm Candidates Today

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

- RSA
  - RSA with SHA-256 (8) – mentioned here for completeness
  - RSA with SHA-512 (10)
- 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)

N.B. Of the algorithms listed above, only algorithms 8, 10 & 13 are currently listed by RFC 8624 as a MUST implement for validators.

Implementation: How to roll

- Out-of-band pre-publication of new Trust Anchor
- Double signatures – both KSK & ZSK – during rollover, no signature pre-publication
- In-band 5011 Algorithm Rollover for introduction of new key and revocation of old key

The algorithm rollover needs to be built around the existing framework used when managing keys for the root zone. The phases used for the normal key rollovers will be adjusted and reused for the algorithm rollover.

Whether to roll the ZSK during the algorithm rollover is TBD.

Rollback plans will be developed and criteria for use defined.

Exact implementation plan defined later by RZM partners.

Testing

- Testing of validating resolver implementations
  - RFC 5011 compliance
  - Validate proposed implementation
- Evaluating operational impact when rolling to currently available algorithms
- A rollover testbed will be set up to test accelerated algorithm rollovers with RFC 5011
  - Public participation to be announced

Related Activities

- Update of RFC 7958 – DNSSEC Trust Anchor Publication for the Root Zone
  - Semantics clarifications
  - PKIX formats (CSR/Certificate) removed
  - OpenPGP signature removed
- Track third party initiatives that measure the algorithm rollover process.
- Update of RFC 8624? – Algorithm Implementation Requirements and Usage Guidance for DNSSEC – to include more mandatory to implement algorithms, e.g. ED25519.

Timeline

	Design Team	KSK
Apr 2023		Generate KSK
Jul 2023	Draft report for ICANN public comment	Replicate KSK
Sep 2023	Final report	
Jan 2024		KSK published in Root Zone
Q4 2025		KSK rollover

Next key generation: Q2 2026
Possible algorithm rollover: Q4 2028

Questions?

Share your questions and insights:

- Contact us at iana@iana.org

More information available at:

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