

Root Zone KSK Update

Kim Davies
March 6, 2024

PTI | An ICANN Affiliate

Objectives

- HSM and KSK Rollover
- Algorithm Rollover

HSM and KSK Rollover

HSM & KSK Rollover - Background

- In Q2 2023 we announced plans to generate a successor KSK and to perform a rollover following the proposed timeline for KSK rollovers that had been published in 2019
- Learned that Ultra are discontinuing the KeyperPlus HSM effective March 2024 with support through March 2025 - this has now been extended to March 2027
- Continued with plans to generate and replicate the KSK while we worked with root zone management partners to assess options
- Announced plans to not publish the new KSK as a trust anchor, effectively halting the existing rollover project, and instead restart the rollover on HSMs from a new vendor

HSM & KSK Rollover - HSM Selection

- Reviewed several vendors against our evaluation criteria - full details are published in the recent announcement. Form factor was an important requirement - at least two units should fit in the equipment safe with room for two Keyper HSMs.
- Scope initially limited to FIPS 140-2 Level 4 HSMs, but widened to include products certified to FIPS 140-3 Level 3 based on the limited number of products on the market.
 - Preference for off the shelf units over bespoke solutions to avoid failure situations being limited to our solution
- Conducted an evaluation of several products, ultimately selecting the Luna USB HSM. Key factors in the decision included the longevity of the vendor, facilitation of transparent operations, and key backup options.

HSM & KSK Rollover - Luna



HSM & KSK Rollover - Timeline

- Our Intention is to generate the new key in Q2 consistent with previously published plan for future rollovers. The motivation for this timeline are:
 - Activation/rollover to occur on 11 October (every three years), providing a predictable schedule for the internet community
 - Lengthy 18 month pre-publication period to accommodate software update cycles
 - Generation, replication, and signing/publication are separate ceremonies aligned with existing quarterly ceremonies to simplify operations and manage costs
- This timing sees the retirement of the Keyper HSMs within our desired operational window of five years.
- Verisign, as root zone maintainer, also need to update their systems to migrate from the Keyper HSMs.

Algorithm Rollover

Algorithm Rollover

- Design team have reviewed public comments and are making minor modifications to the document. Expect the final report in Q2.
- Plan to continue with the normal KSK rollover to prioritize moving off the Keyper HSM hardware.
- Algorithm rollover in the root is more complex:
 - Queries for non-existent domains (~50% queries) could switch to TCP
 - To mitigate operational load expect temporary reduction in size of the RSA ZSK (e.g. to 1536 bit)
 - Full operational plans to be developed
 - Updates required for both software and processes
 - Update the trust anchors of all validating resolvers
 - Expect community consultation on the algorithm selection
- Provisionally expect the rollover to occur in 2029 if following the idealized three year KSK lifecycle. Key may be generated earlier to allow sufficient time for out-of-band distribution and testing.