2024 Hardware Security Module Replacement

Executive Summary

The Internet Assigned Numbers Authority (IANA) utilizes Hardware Security Modules (HSMs) for securely storing the Root Zone Key Signing Key (KSK). After learning its current equipment manufacturer will no longer produce the existing HSMs being used, the Thales Luna USB Hardware Security Module (HSM) 7 has been identified as the preferred replacement. To introduce this new HSM, a Root Zone Key Signing Key (KSK) rollover will be performed using the current RSA with SHA-256 algorithm. This work is proposed to begin in the second quarter (Q2) of 2024 with the rollover to occur in October 2026.

Introduction

IANA uses cryptographic materials stored in hardware security modules (HSMs) for Root Zone Key Signing Key (KSK) ceremonies.

In April 2023, IANA became aware of the decision by the manufacturer of the Keyper PLUS HSM – the equipment used to store private key materials for the Root Zone KSK – to cease its production of the device.[1] Furthermore, the manufacturer will offer no successor product.

The Keyper products we use were the only viable devices at the time of selection that met the Federal Information Processing Standard (FIPS) 140-2 Level 4 overall certification, which at the time, was the highest possible security level for any HSM. This maximal security level was thought to be the strongest option for both security outcomes and trust in the system. After selecting this HSM, operating procedures were tailored to its unique features. The HSMs do not provide a function that would allow the private key to be exported and imported into alternative vendors' HSM devices.

As a result, a decision has been taken to move operations to a new model of HSM from a different vendor. Because the KSK is not exportable, the remediation plan necessarily requires a KSK rollover in tandem with the hardware change. A new KSK would be generated on the newly selected platform — the Thales Luna USB HSM 7. The current algorithm (RSA SHA-256) will be used in the new key, and a KSK rollover will be conducted to the new key.

The rollover of the Root Zone KSK requires coordination among a wide variety of Internet stakeholders, from the Internet Corporation for Assigned Names and Numbers (ICANN), IANA,

[1] https://www.ultra.group/media/3747/20230306-end-of-life-notice-for-ultra-keyperplus.pdf

and the Root Zone Maintainer, to the implementers and operators of every validating resolver on the Internet.

This rollover will be the second rollover of the Root Zone KSK and the first since the publication of the Proposal for Future Root Zone KSK Rollovers[2]. This project will conduct a rollover that takes reasonable measures to propagate the new key in advance of the rollover date, minimizing potential disruptions to Internet operability. This rollover will also supplant the KSK rollover process begun using the current Keyper hardware in April 2023.

High-Level Timeline

The planned introduction of new HSMs in 2024 Q2 is an aggressive timeline. This is driven by two factors: the intention to follow the proposed schedule for KSK rollovers, giving sufficient time to stakeholders to prepare for the rollover with a lengthy, pre-publication phase and to ensure that the replacement of the end-of-life Keyper HSMs are within their desired operational lifetime.

The proposed HSM and KSK rollover is anticipated to follow the timeline below.

Quarter	**Activity**
2024 Q2	Generate the 2024 KSK in the new Thales Luna USB HSMs in KMF East
2024 Q3	Replicate the KSK 2024 in the new Thales Luna USB HSMs at KMF West and publish the 2024 KSK in the DNS Root Trust Anchors file
2024 Q4	Outreach and communications
2025 Q1	The 2024 KSK first appears in the DNS Root Zone. Outreach and communications are conducted
2025 Q2 – 2026 Q3	The 2024 KSK continues to be published in the root zone. Outreach and communications are conducted
2026 Q4	Conduct the second KSK rollover to KSK 2024
2027 Q1	Revocation of the 2017 KSK
2027 Q2	Destruction of the 2017 KSK, destruction of 2023 KSK (which was generated but never used in production), and destruction of Keyper HSMs in KMF East
2027 Q3	Destruction of the 2017 KSK, destruction of the 2023 KSK, and destruction of Keyper HSMs in KMF West

[2] https://www.icann.org/en/system/files/files/proposal-future-rz-ksk-rollovers-01nov19-en.pdf

Selection Criteria

IANA performed an initial evaluation of several HSMs based on the criteria described below:

- An HSM that is validated FIPS 140-2/-3 level 4 overall
    - Validation to level 3 overall was also considered, on the basis that any perceived gaps could be addressed with compensating controls
- An HSM that can remain in storage without external power and for extended periods without losing the key material
- An HSM that is suitable for storage in a GSA class 5 size IV safe enclosure, mindful of our operational environment and the space constraints within
- An HSM that has desirable indicators for transparency during operation, for example, an LCD display
- An HSM that has desirable connection interfaces, for example, serial port, ethernet port, or USB port
- An HSM that has desirable input devices like a keypad or smartcard reader
- An HSM that supports quorum with M-of-N multifactor authentication for configuration, operation, and backups
- An HSM that supports PKCS#11
- An HSM that supports various cryptographic algorithms expected to be needed
- An HSM that supports key backups preferably to smartcards or similarly secure media
- An HSM that provides usage logs for record and audit keeping
- An HSM manufactured by a company with a solid reputation and long term viability

Following an initial evaluation, IANA selected the Thales Luna USB HSM 7 and the Utimaco CSe PCI card with Enclosure for further testing within the parameters and procedures of the KSK ceremony.

Selection and Impact

IANA identified the Thales Luna USB HSM 7 as best suited for our requirements. While both the Luna and Utimaco were deemed suitable, the transparency provided by the built-in LCD and the backup to a dedicated HSM were key differentiators in our choice.

All evaluated HSM differed in their implementation of the criteria, and that difference is also notable when compared to that of the Keyper Plus HSMs. The current design and format of the ceremony has been influenced by and tailored to work with the Keyper Plus.

Notable changes are identified below:

Authorization: The Keyper Plus HSMs have distinct keys for the authorization and backup key encryption functions. The Thales Luna USB HSM 7, however, has one domain key that covers both the authorization and key backup functions. The impact of this change is that the

authorization credentials in KMF East will be identical to the authorization credentials in KMF West. We consider this change acceptable given the existing physical controls, specifically the safety deposit box keys, continue to tie individual Cryptographic Officers (COs) to a single facility.

By design, all desired credential sets must be generated in sequence during the instantiation of the new hardware. Cloning the original credential sets may be performed to create copies of previously created credential sets at any time in the future. This feature suggests that credential sets for all Trusted Community Representatives (TCRs) and roles should be performed in the first ceremony where the new hardware is introduced.

Key backup: The Thales Luna USB HSM 7 backups are performed exclusively to a dedicated Luna Backup HSM. These backup HSMs will be kept in the equipment safe as with the current backup copies.

All TCRs, including the Recovery Key Share Holders (RKSHs), will be assigned full sets of credentials. The full sets of credentials will comprise CO, SO, Audit, and Domain credential types. COs will continue using the minimum threshold of 3 of 7, and for RKSHs the threshold of 5 of 7 to make a quorum, respectively. Due to the design of the Thales Luna USB HSMs, both CO and Domain credential types are required to perform HSM backups, and all credential types needed for projected recovery scenarios. The following table displays each credential type and its purpose in brief:

Type	Purpose
CO	Required to perform key operations or access a key for backup operations
SO	Required for administration of the HSMs
Audit	Required to access transaction logs from the HSMs
Domain	Facilitates encrypted transfers to dedicated Luna backup HSMs

Supported Algorithms:[3] The Thales Luna USB HSM 7 has full suite B algorithm support and the current firmware version (7.7.2) has cryptographic support for the following major DNSSEC algorithms:

- RSA 2048-4096 bit with SHA-256 (algorithm 8) (FIPS mode)
- ECDSA Curve P-256 with SHA-256 (algorithm 13) (FIPS mode)
- Ed25519 (algorithm 15) (not in FIPS mode)

[3] https://thalesdocs.com/gphsm/luna/7/docs/usb/Content/sdk/usb_mechanisms/mechanism_summary_usb_7-7-2.htm

In-process FIPS validation: The FIPS 140-3 Level 3 Overall certification for the Thales Luna USB HSM 7 Cryptographic Module is currently in review as of 16 February 2024.[4] IANA believes it acceptable to generate and replicate keys on this device while it awaits validation, based on the assumption that the certification for the device and its operational firmware is issued prior to the key's operational use. IANA considers this a low risk given the vendor's reputation.

FIPS 140-3 Level 3: The DNSSEC Practice Statement (DPS) requires that the Key Signing Key (KSK) is used within HSMs validated to FIPS 140-2 Level 4.[5] This specification was superseded by FIPS 140-3 which has different definitions for the levels of conformance. A detailed breakdown of the changes between FIPS 140-2 and FIPS 140-3 is below.

IANA believes that the main difference between FIPS 140-3 Level 3 and Level 4 physical security of cryptographic modules is the addition of active tamper monitoring. Active tamper monitoring will detect when intrusion attempts are made to the physical case of the HSM and tamper/zeroize the unit, even when the HSM is offline or powered off. A constant power source is required for active tamper monitoring. Reliance on long-life batteries can be a single point of failure.

Upon consideration of disaster scenarios where our facilities were physically compromised to the point of physical access to the HSMs, our response would be identical in the case of a FIPS 140-3 Level 3 or Level 4 certified HSM. Pursuant to that, it is the opinion of IANA that additional compensating controls are redundant in conjunction with the migration to Thales Luna USB HSM products.

[4] https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List
[5] https://www.iana.org/dnssec/procedures/ksk-operator/ksk-dps-20201104.html#section-5.2.1

FIPS Validation

Please note that the following information has been summarized, digested, and processed with the intention of clarifying this document. Please refer to the United States National Institute of Standards and Technology's (NIST) website for reference https://csrc.nist.gov/Projects/cryptographic-module-validation-program.

FIPS 140-2 v.s. 140-3

FIPS 140-3 supersedes FIPS 140-2, introducing some significant changes. Unlike the FIPS 140-2 Standard, which included the requirements for cryptographic modules, FIPS 140-3 references ISO/IEC 19790:2012. The testing for these requirements will be in accordance with ISO/IEC 24759:2017. NIST also introduced to its Special Publications, the SP 800-140 series, that modify ISO/IEC Standards.

FIPS 140-2 modules can remain active for five years after validation or until 21 September 2026, when the FIPS 140-2 validations will be moved to the historical list. Even on the historical list, the Cryptographic Module Validation Program supports the purchase and use of these modules for existing systems.[6]

The standard FIPS 140-2/-3 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover a wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operating environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

Each area allows for increasing levels of security with cumulative security requirements for each security level. In these areas, the cryptographic module will receive a rating that reflects the maximum security level for which the module fulfills all of the requirements of that area. In areas that do not provide for different levels of security (i.e., standard set of requirements), the area will receive a rating commensurate with the overall security level of the module.

The following table summarizes the cryptographic module requirements for each of the applicable FIPS validation levels of both 140-2 and 140-3. Note, the ISO/IEC Standards describing these requirements can only be accessed after purchase and may not be reproduced. After comparison, it became apparent that a previous draft version of the FIPS 140-3 was very close to the final, and we used the Special Publication to fill the gap.

[6] https://csrc.nist.gov/Projects/fips-140-3-transition-effort

FIPS 140-2[7] Security Requirements	140-2 Level 4	FIPS 140-3[8][9] Security Requirements	140-3 Level 3	140-3 Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.	**1. Cryptographic Module Specification**	Specification of module, cryptographic boundary, Approved and Allowed algorithms and key establishment methods and Approved modes of operation. Description of module hardware, software and/or firmware. Module documentation. Module indication of Approved mode of operation.	
Cryptographic Module Ports and Interfaces	Data ports for unprotected critical security parameters logically or physically separated from other data ports.	**2. Cryptographic Module Interfaces**	Required and Optional Interfaces. Specification of all interfaces and of all input and output data paths. Trusted Channel.	
Roles, Services, and Authentication	Identity-based operator authentication.	**3. Roles, Services, and Authentication**	Identity-based operator authentication	Multi-factor authentication.
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.	**-**	This section has been moved to section 10. Life-Cycle Assurance	
Physical Security	Tamper detection and response envelope. Environmental Failure Protection (EFP) or Environmental Failure Testing (EFT)	**6. Physical Security**	Environmental Failure Protection (EFP) or Environmental Failure Testing (EFT)[10] Tamper response and zeroization circuitry on removable covers and doors. Protection from probing from module openings. Hard opaque coating or enclosure.	Environmental Failure Protection (EFP)[11] Tamper detection and zeroization circuitry for multi-chip modules. Fault Injection Mitigation.
Operational Environment	Referenced Common Criteria (CC) Protection Profiles (PPs) plus trusted path evaluated at EAL4.	**5. Operational Environment**	(non-modifiable) Operational environment components bound to the firmware module. (limited) Controlled loading of additional through the Software/Firmware Load Test.	

[7] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
[8] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
[9] https://csrc.nist.gov/files/pubs/fips/140-3/2pd/docs/fips140-3-draft-2009.pdf
[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140.pdf (AS07.77 and AS07.81)
[11] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf (page 11)

Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization. Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	**8. Sensitive Security Parameter (SSP) Management**	Requirements for Random Bit Generators, SSP generation, SSP establishment, SSP entry and output, SSP storage, and Critical Security Parameter (CSP) zeroization. Electronically transported CSPs entered or output only encrypted. Trusted Channel required. Manually transported SSPs entered or output either in encrypted form or using split-knowledge procedures, regardless of the entry or output method (manual or electronic).	
EMI/EMC	EMI/EMC: 47 CFR FCC Part 15. Subpart B, Class B (Home use).	**-**	Electromagnetic Interference / Electromagnetic Compatibility These requirements have been removed	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.	**9. Self-Tests**	Pre-operational self-tests: software/firmware integrity test, bypass test and critical functions tests. Conditional self-tests: cryptographic algorithm test, pair-wise consistency test, software/firmware load test, manual key entry test, conditional bypass test and critical functions test. Cryptographic algorithm tests specified in Annexes A through E. Pair-wise consistency test for key pairs entered into module. Periodic self-tests.	
Design Assurance	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.	**10. Life-Cycle Assurance**	Configuration Management: Automated configuration management system. Design: Detailed design for testing all security services. FSM: Finite state model. Development: Software high-level language. Hardware high level descriptive language. Vendor Testing: Low-level Testing. Delivery and Operation: Delivery Procedures. Guidance Docs: Administrator and non-administrator guidance.	Configuration Management: Automated configuration management system. Design: Detailed design for testing all security services. FSM: Finite state model. Development: Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed. Vendor Testing: Low-level Testing. Delivery and Operation: Operator authentication using vendor provided authentication information. Guidance Docs: Administrator and non-administrator guidance.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.	**11. Mitigation of Other Attacks**	Documentation of the mitigated attacks not defined in the standard.	Documentation includes the methods used to mitigate attacks, and the methods/requirements to test the effectiveness of mitigation techniques.
		(New) 4. Software/Firmware Security	Approved digital signature based integrity test	
		(New) 7. Non-invasive Security	Review of documented mitigation techniques against applicable noninvasive attacks listed in Annex F (mandatory for single-chip cryptographic modules and optional for all other hardware module embodiments).	Mitigation against noninvasive attacks with specific test requirements for this security level, specified by the validation authority (mandatory for single-chip cryptographic modules and optional for all other hardware module embodiments).

Future Considerations

If an HSM with more appealing attributes becomes available in the future, we can employ a similar HSM introduction with a key rollover strategy to integrate these units into KSK operations.

Impact on the Root DNSSEC Operations

We do not anticipate any major impact to Root DNSSEC design and operations:

- Current security and operational design will be maintained
    - Credential safe will contain current and new credentials
    - Equipment safe will contain current and new hardware
    - Security of credentials and hardware will be safeguarded at the current level
- Current TCR quantity and roles will be maintained with 7 COs per KMF (14 total) and 7 Recovery Key Share Holders (RKSHs)
    - COs will maintain the 3 of 7 quorum threshold for credentials
    - RKSHs will maintain the 5 of 7 quorum threshold for credentials

Instantiation of new HSM hardware during KSK Ceremony in 2024 Q2

We plan to perform the instantiation of the new HSM hardware in KMF East one day before or after the standard KSK Ceremony 53:

- Duplicate credential sets generated for the new hardware can only occur during the time of the original credential set's creation. A duplicate set cannot be created at a later time; and, therefore, an instantiation will require:
    - All East-Coast COs to participate in person
    - All RKSH to participate in person
    - All West-Coast COs may, optionally, participate remotely
- KSK-2024 generation
- Backup generation

Instantiation of new HSM hardware during KSK Ceremony 54 in 2024 Q3

We plan to perform the instantiation of the new HSM hardware in KMF West one day before or after the standard KSK Ceremony 54:

- Credential distribution:
    - All West-Coast Crypto Officers to participate in person
- Restore the 2024 KSK backup to production HSMs and test credentials

Continuing work

Root Key Operations Security (RKOS) requires completing the following work prior to implementation:

- Documenting updates, specifically the DPS, and policy and procedure documents
    - RKOS notes that FIPS requirements in the DPS should be updated prior to key generation, with other procedures updated prior to operationalization of the key
- Software development – minor changes will be required for the software to support dual key signing with the Keyper Plus and Thales Luna USB HSM 7s
    - These changes are neither required for key generation nor replication, and will be completed well before the forecasted initial signing

Alternative options

Here are the alternate options considered, and the primary considerations for why they may be desirable and why they were ultimately not recommended:

- **Retain using the HSM Keyper.** IANA has acquired a number of additional units that would allow the continued use of the Keyper for many years to come. However, the vendor has stopped producing the units and support for these units is expected to end. IANA does not believe it is prudent to continue to rely on these devices any longer than necessary for these reasons.

- **Perform the rollover events at different dates.** IANA has an ambition to standardize the cadence of rollovers so they are consistently applied. The current approach sees a generation event occur in Q2 of a calendar year, with production usage beginning two and a half years later in Q4 of that calendar year. The actual rollover happens on the 11th day of the calendar quarter, resulting in a rollover on 11 October. Delaying the generation even one more quarter beyond Q2 of 2024 would provide additional time for preparation and research. But, this was considered undesirable, because the key rollover is an event requiring global coordination for which predictability is preferred.

Credentials: Keyper and Thales Luna G7

Credential Types and Functional Descriptions

Keyper

Role	Purpose
OP (Operator)	Configures the HSM to an online or offline state allowing/disallowing communication through its ethernet adapter. Required for communication with the laptop for key signing operations.
SO (Security Officer)	Used for HSM administrative operations. Required to create all other role smartcards (OP, CO, SMK, etc) and the introduction and zeroization of a new HSM.
CO (Crypto Officer)	Used for the key management functions in the HSM. Required for adding or deleting keys stored in an HSM.
SMK (Storage Master Key)	Allows an HSM to read an encrypted APP key backup. Required for migrating keys and disaster recovery.
AAK (Adapter Authorization Key)	Configures an HSM to accept existing OP, CO, and SO smartcards previously generated in a different HSM. Required for the introduction of a new HSM.
APP (Application Key)	An encrypted backup copy of the keys stored in an HSM which can only be decoded by its corresponding SMK. Required for migrating keys and disaster recovery.

Thales Luna

Type	Purpose
CO (Crypto Officer)	Used for the key management functions in the HSM. Required for adding or deleting keys stored in an HSM.
SO (Security Officer)	Required for administration of the HSMs
Audit	Required to access transaction logs from the HSMs
Domain	Associates HSMs to facilitate cloning key materials between Thales Luna HSMs and Thales Luna Backup HSMs