

Luna T-Series Hardware Security Modules

Cipher Summit 2025

Thales Trusted Cyber Technologies

Table of Contents



HSMs, the Root of (Zero) Trust



Luna T-Series HSM Family



Luna T-Series Mini HSM Announcement



Planting Roots of Trust

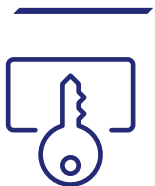


Post-Quantum Cryptography

HSMs, the Root of (Zero) Trust



HSMs are the Foundation of Trust, Securing the Keys to Your Data



A Root of Trust is the foundation of a cryptographic system



Digital security is dependent on cryptographic keys that encrypt and decrypt data and perform functions such as signing and verifying signatures



Ensuring the integrity of those keys and the cryptographic functions within a secure environment such as an HSM is paramount



A Root of Trust safeguards the security of data, users, and applications and helps to build trust in the overall ecosystem

HSMs:
The foundation of digital trust

Luna HSMs Protect Traditional and Emerging Cryptographic Needs

Traditional



Secure **digital signatures**



Secure **PKI** root keys

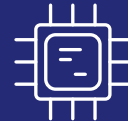


Ensure software remains secure, unaltered and authentic with **code signing**



Ensure key ownership in the **cloud**

Emerging



Protect your post **quantum** crypto



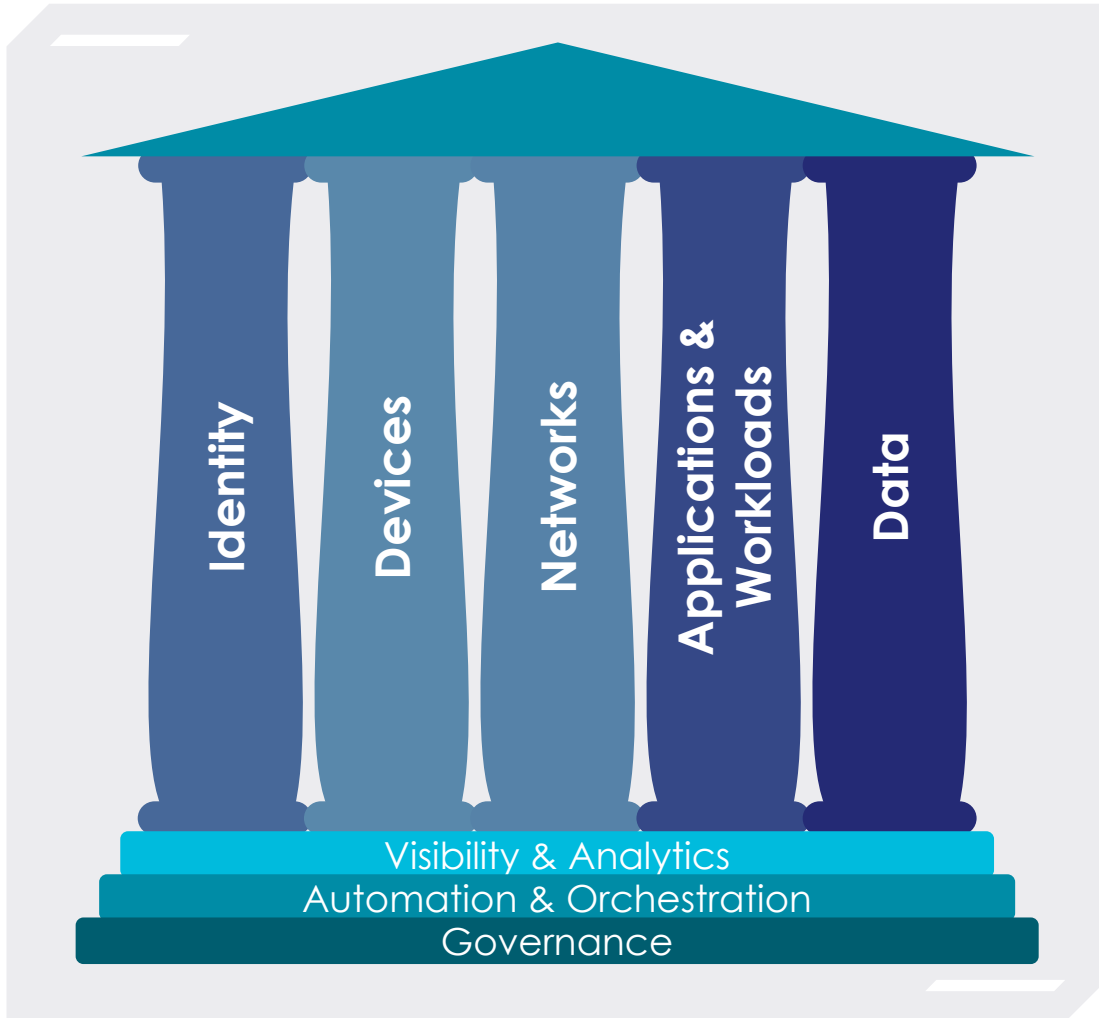
Building a **Zero Trust** Network



Create secure digital identities for **IoT** and **secure manufacturing**



Protect **Non-Person Entity** and **AI Agent** identities



Zero Trust Reference Architecture

A FIPS 140 Level 3 HSM is a foundational component to all pillars of ZT

- ▶ Protecting **User** identities at the PKI root
- ▶ Generating secure TLS keys for **Network** traffic
- ▶ Generating secure **Device** identities
- ▶ Protecting **Workloads** with secure code signatures
- ▶ Providing key material and entropy for **Data** encryption



Luna T-Series HSM Family

Thales TCT Luna HSM Family



Luna Network HSM

T-2000 & T-5000

Network-attached HSM that protects encryption keys used by applications in on-premise, virtual, and cloud environments

Typical use cases

PKI, SSL/TLS, Code Signing, Cert Signing & Validation, Doc Signing, Transaction Processing, DB Encryption, Smart Card Issuance



Luna as a Service

Dedicated & Managed



FedRAMP

Cloud-based HSM delivered through XTec's FedRAMP High authorized AuthenX Cloud

Typical use cases

Cloud Smart Root-of-Trust, Anchoring applications across multiple cloud providers



Luna PCIe HSM

T-2000 & T-5000

Embedded HSM that protects cryptographic keys and accelerates sensitive cryptographic operations

Typical use cases

Securing Custom Applications



Luna Tablet HSM

Backup & USB HSM

USB-attached HSM that is ideal for storing root cryptographic keys in an offline key storage device.

Typical use cases

Root CAs

Why Choose Luna T-Series HSMs



Security & Compliance

Address compliance requirements with FIPS 140-2 L3 and CNSS Approval

Keys and certificates automatically generated and stored in hardware

Quantum Enhanced Keys generated using onboard Quantum RNG



Security First Company

U.S. Foundation (development, manufacturing, personnel, facilities)

Strong security practices



Government Approval & Reference

CNSS approval for TCT HSMs on National Security Systems

NCCoE reference architecture for TLS Server Certificate Management

Trusted supplier to U.S. Govt.



Scalability and High Availability

Ability to have multiple applications share the same hardware

Easy to add new applications – no new HSM required

Ability to cluster HSMs to avoid single point of failure



Partner Ecosystem

Out-of-the-box integrations with their applications

Existing integrations that align with partner's future plans

Announcing: Luna T-Series Mini HSM

Luna T-Series at the Edge



Luna T-Series Mini HSM
Launching: Winter 2025

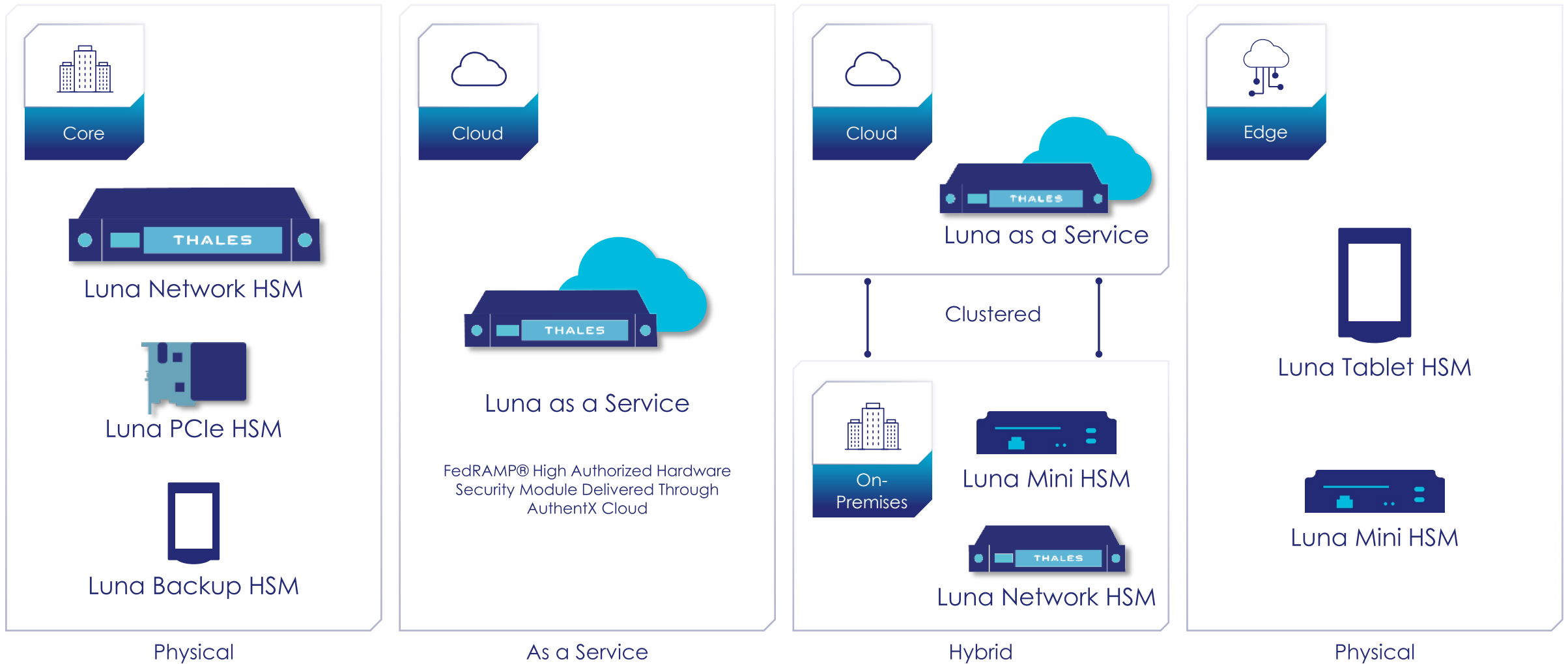
Luna T-Series Tablet HSM
Launched: 28 Aug 2024



7th Generation Crypto Module
Common Luna T-Series Platform
USB or Ethernet Connectivity
Modern Authentication Ready
Backup Configuration Available
Ruggedized Enclosure per MIL-STD-810H

Planting Roots of Trust

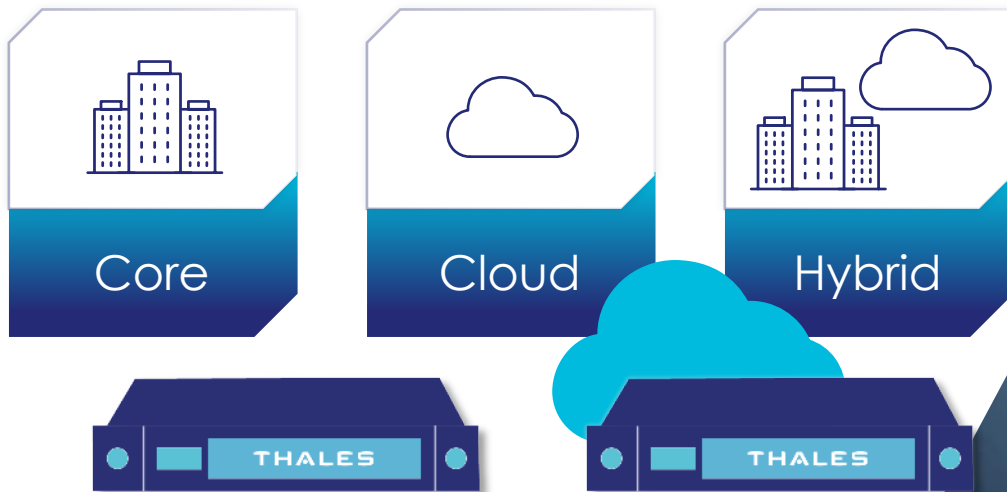
Roots of Trust Anywhere You Need One



Federal PKI & Credentialing

CAC and PIV credentials are built on HSM-rooted card management and identity systems

Luna T-Series HSMs are CNSS approved for use in national security systems PKI

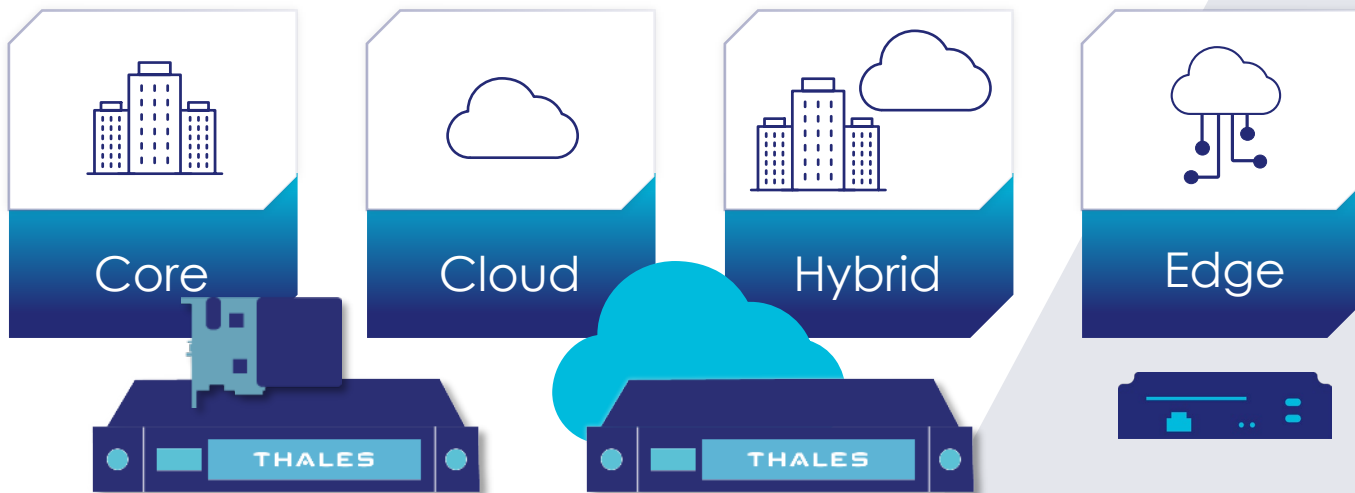


CipherTrust Data Security Platform

Luna T-Series HSMs hold CipherTrust's master keys for higher assurance

Provides FIPS-validated QRNG or RNG, improving entropy for all keys

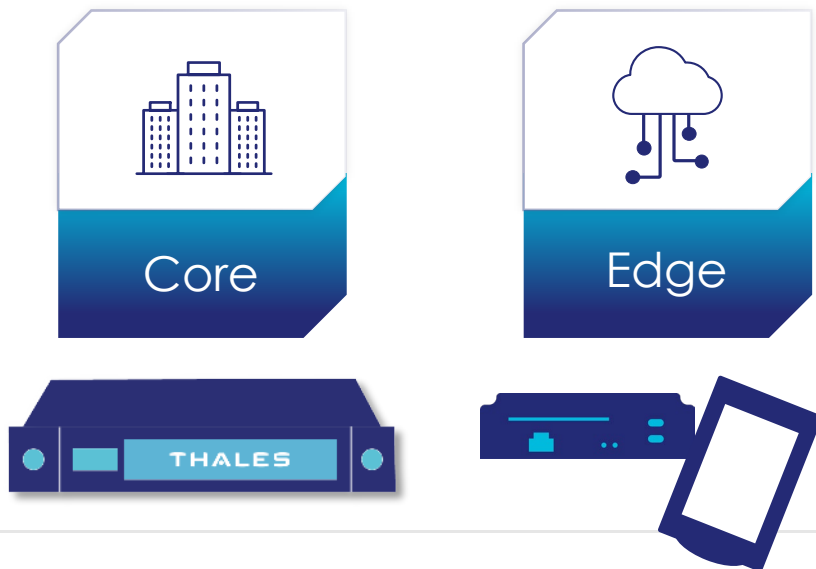
Supports both physical and virtual CipherTrust Manager appliances



CSfC Deployments

Luna T-Series HSMs fulfill the Key Management Requirements Annex specs for hardware roots of trust

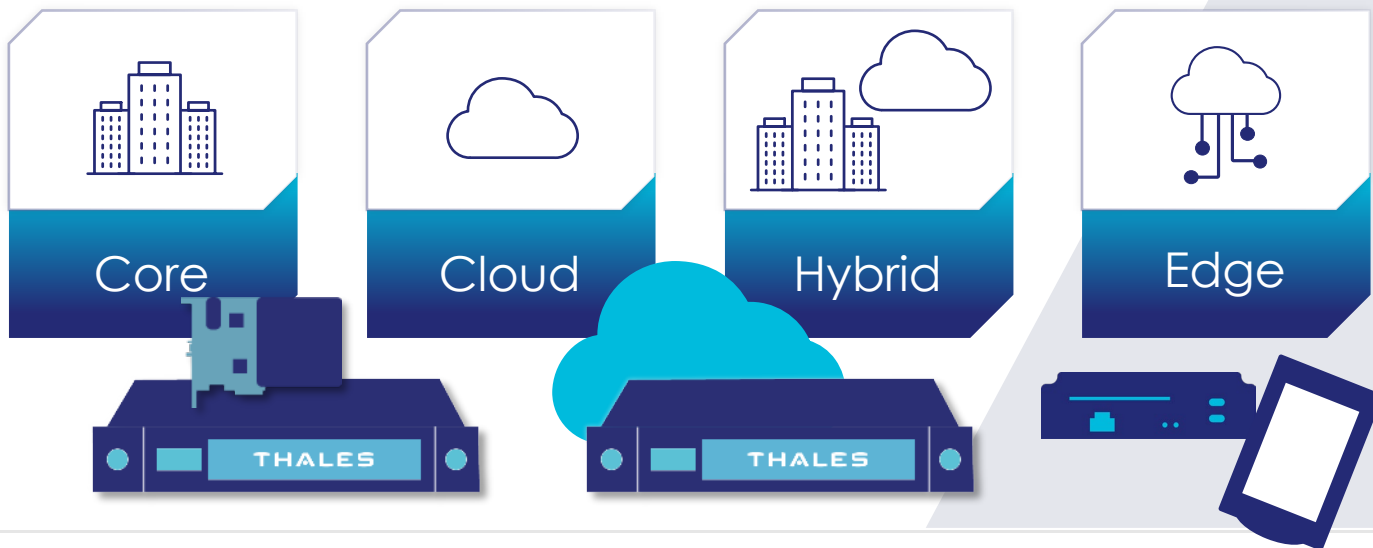
Luna T-Series HSMs are CNSS approved for use in national security systems PKI



Post-Quantum Code Signing

Luna T-Series supports SP800-208
and CNSA 2.0 requirements for
LMS, HSS, and ML-DSA

Facilitates a crypto agile
approach to migrate to PQC



Post-Quantum Cryptography

NCCoE “Migration to Post-Quantum Cryptography” Project



> NIST’s engagement with the community to address issues related to PQC migration

- Now the largest NCCoE project with >40 collaborators from government, industry and financial sectors

> Thales was a founding participant in June 2022

- Thales HSMs one of six HSM vendors performing PQC interoperability testing (2023)
 - Accelerated Thales TCT T-Series HSM release of pre-standards PQC in July 2023
 - Results published in NIST SP 1800-38 (Draft)

> Adding Thales PQC smartcards to interoperability tests in 2025



MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

BACKGROUND

The advent of quantum computing technology will render many of the current cryptographic algorithms ineffective, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to adversaries. It is essential to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

GOAL

The initial scope of this project will include engaging industry to demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes. Once the public-key cryptography components and associated assets in the enterprise are identified, the next project element is prioritizing those applications that need to be considered first in migration planning. Finally, the project will describe systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across different types of organizations, assets, and supporting technologies.

CHALLENGES

- Organizations are often unaware of the breadth and scope of application and function dependencies on public-key cryptography.
- Many, or most, of the cryptographic products, protocols, and services on which we depend will need to be replaced or significantly altered when post-quantum replacements become available.
- Information systems are not typically designed to encourage supporting rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure—requiring intense manual effort.
- The migration to post-quantum cryptography will likely create many operational challenges for organizations. The new algorithms may not have the same performance or reliability characteristics as legacy algorithms due to differences in key size, signature size, error handling properties, number of execution steps required to perform the algorithm, key establishment process complexity, etc. A truly significant challenge will be to maintain connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms.


BENEFITS

The potential business benefits of the solution explored by this project include:

- helping organizations identify where, and how, public-key algorithms are being used on their information systems
- mitigating enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/updating hardware, software, and services that use PQC-vulnerable public-key algorithms
- protecting the confidentiality and integrity of sensitive enterprise data
- supporting developers of products that use PQC-vulnerable public-key cryptographic algorithms to help them understand protocols and constraints that may affect use of their products

DOWNLOAD PROJECT DESCRIPTION

This fact sheet provides a high-level overview of the project. To learn more, visit the project page: <https://www.nccoe.nist.gov/crypto-ability-considerations-migrating-post-quantum-cryptographic-algorithms>



HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the project's Community of Interest, please email applied-crypto-pqc@nist.gov

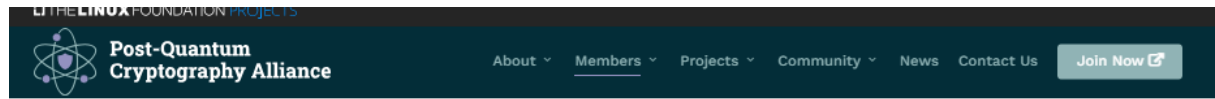
Thales TCT & NSA Sign PQC Cooperative Research and Development Agreement (CRADA)

CRADA for evaluating the NIST selected PQC algorithms when operating on an HSM

CRADA results will be used:

- By Thales TCT to accelerate PQC algorithm deployment
- Assist the Government and other HSM users in understanding the value of using PQC enabled HSMs to mitigate the quantum threat

Premier Member of Post-Quantum Cryptography Alliance



Members

Premier



General



Associate



Post-Quantum Cryptography Alliance

To advance the adoption of post-quantum cryptography, by producing high-assurance software implementations of standardized algorithms, and supporting the continued development and standardization of new post-quantum algorithms with software for evaluation and prototyping.



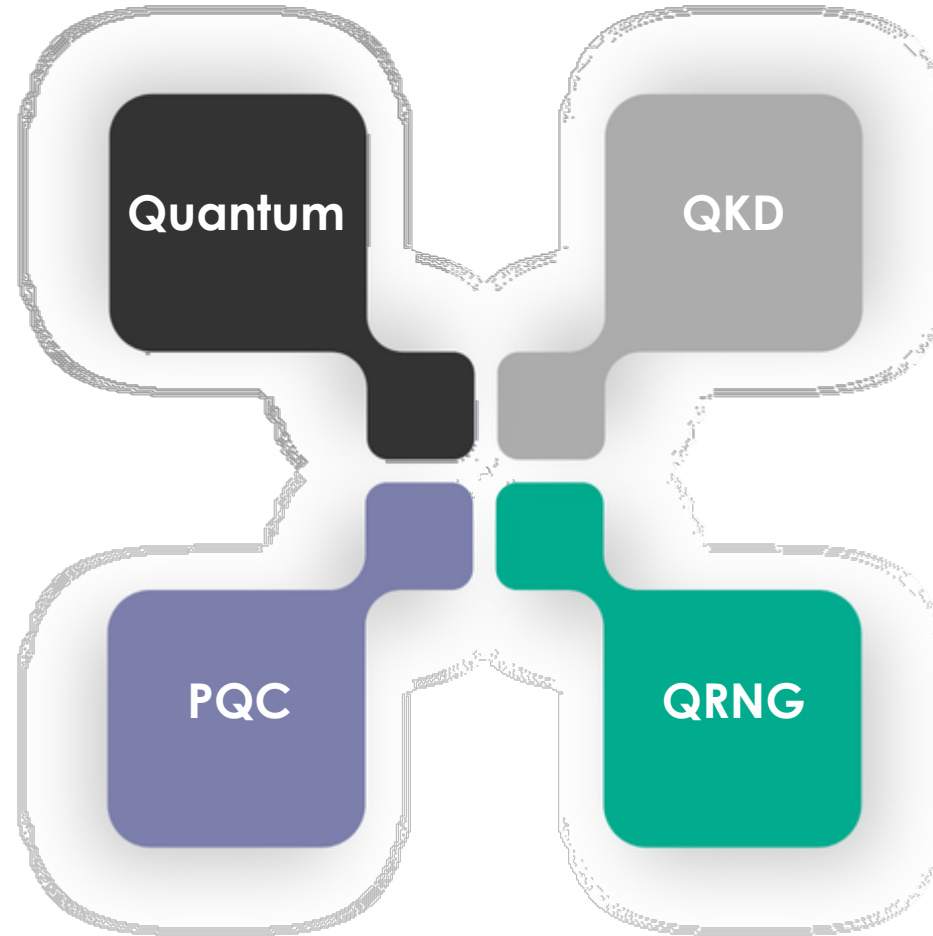
“Which” Quantum?

Quantum Computing

Computer that seeks to exploit the properties of quantum mechanics to speed up computing

Post-Quantum Cryptography (PQC)

Cryptographic systems that are secure against both quantum and classical computers (aka Quantum Resistant Algorithms (QRA))



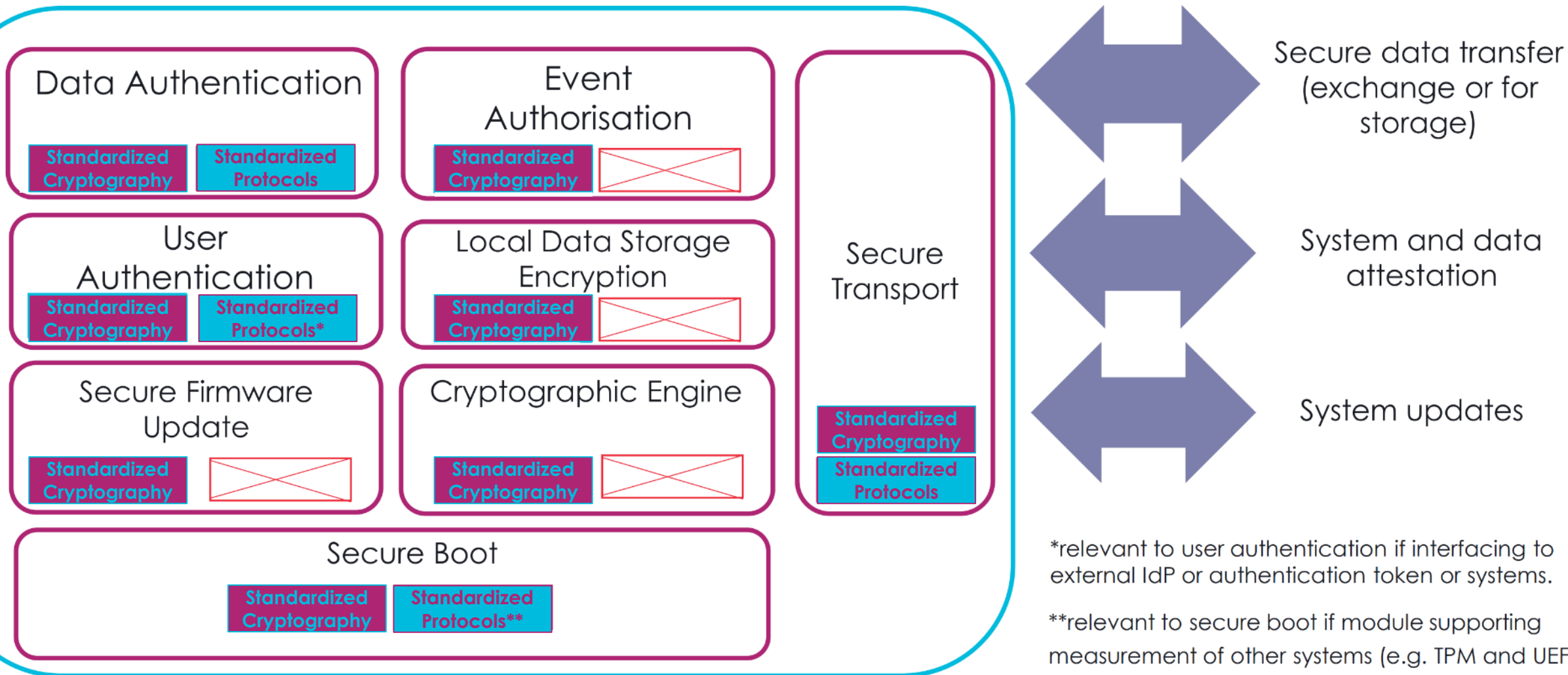
Quantum Key Distribution

Use of quantum physics to distribute keys

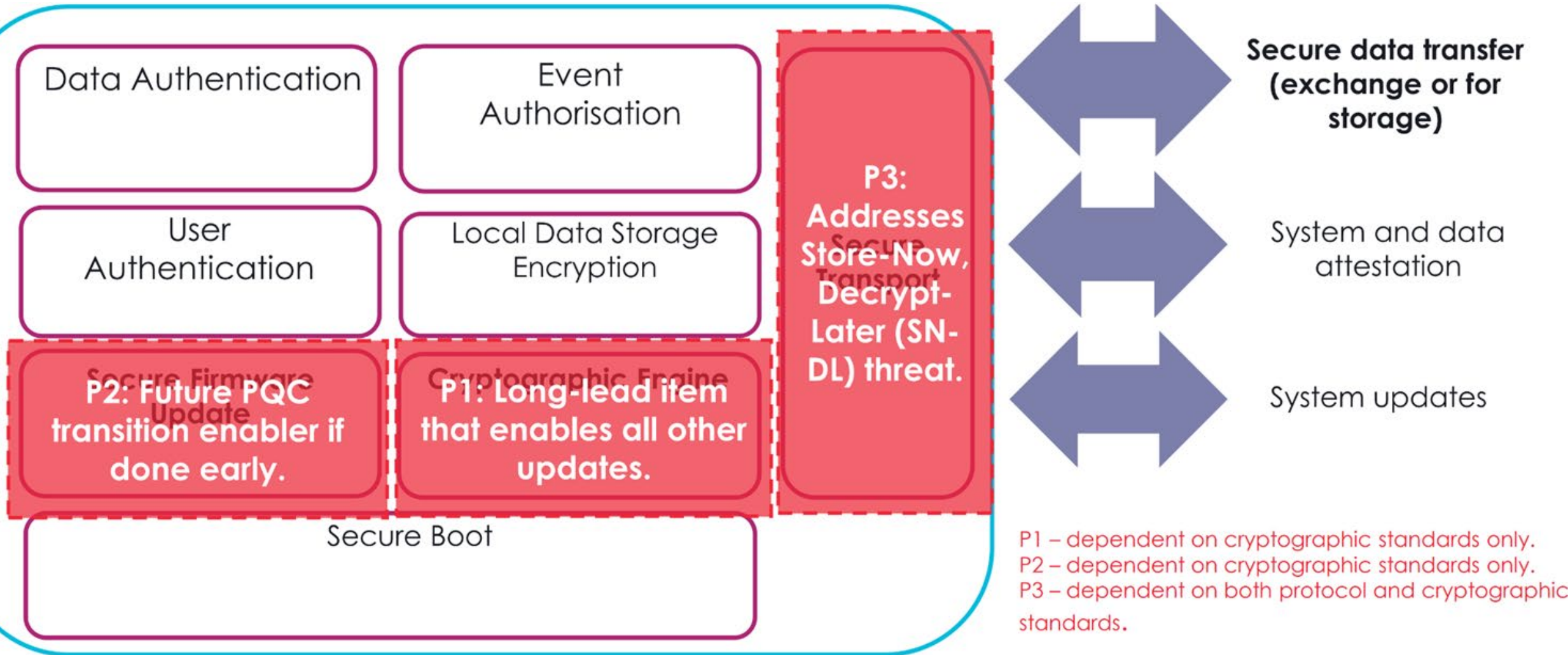
Quantum Random Number Generation

Hardware random number generators used to generate nondeterministic randomness

Anatomy of a Crypto Module



Prioritizing the PQC Transition





HSMs Live in an Ecosystem

- > Cryptographic modules are apex products
- > Protocols and crypto need to be updated at both ends of an integration
- > Integrations at scale rely on standardized APIs
- > Many partners blocked by their dependencies, e.g.:
 - Production quality open-source/COTS software crypto libraries
 - Quantum-safe TLS 1.3 implementations
 - Quantum-safe certificate authorities

Luna T-Series HSM Roadmap

7.15.0

2Q2025

First release with standards-based PQC algorithms for application use:

- ML-DSA
- ML-KEM

FIPS 140-3 update for T-Series

7.15.1

4Q2025

Internal quantum-resistance:

- PQC-signed FW & SW updates
- Quantum resistant cloning

Luna T-Series Mini HSM



7.15.2

2026

External quantum-resistance:

- NTLS
- SSH, SFTP, REST
- Java, KSP, pycryptoki

Modern Authentication

- PED Replacement for MFA
- Quorum for Password Auth

FIPS 140-3 update for T-Series



Thank you!

Evan Pelecky

Senior Product Manager
Cryptographic Key Management

 **443-484-7076**

 **evan.pelecky@thalestct.com**