THALES
Building a future we can all trust

Partner CONNECT

How to sell more HSMs

John Ray
Director, HSM Product Management
www.thalesgroup.com

We evolve with crypto standards – so you stay agile and secure

Latest Crypto Standards: Luna HSMs have continued to meet evolving cryptographic and market needs.

Smooth Migration: easily migrate legacy key materials and create new ones.

Crypto Agility: enable you to quickly adapt to changing business security requirements.

1994	2002	2007	2010	2017	Future
First Luna HSM (G1) created for government and PKI use	Launch of the first **Network HSM (Luna SA Network HSM**) that had multiple applications and could run and be accessed from anywhere	**Luna SA 4** released with a redesigned hardware that was smaller in size than previous generation HSMs and provided an improved performance	**Luna SA 5/6** launched with updated and more robust hardware that provided faster cryptographic performance and enhanced algorithm support while offering more flexible roles for management	**Luna 7** launched with a 10x faster speed than Luna SA 6 and it provides industry leading security, common FIPS certifications across models and a range of model tiers to choose from	LOADING..... Next-Generation Luna HSM

Choose from a variety of HSM options

Network HSM

Highly available and scalable

High-assurance, FIPS 140-3 Level 3 validated, tamper-resistant network connected HSM appliance

Typical use cases
Sub-CA key store(s)
SSL/TLS handshake
Database encryption
Code/Doc signing
Shared HSM access

Cloud HSM Service

Just click and deploy

Cloud-based HSM services to protect critical keys and to accelerate sensitive cryptographic operations across a wide range of security applications

Typical use cases
Sub-CA key store(s)
Database encryption
Code/doc signing
Shared HSM access

Card HSM

Embedded cryptographic processor

High assurance, FIPS 140-3 Level 3 validated embedded PCIe card

Typical use cases
Bundled solution offering applications that require dedicated HSM performance

Small Form Factor HSM

Offline Key Archive & Starter HSM

Small form-factor USB connected Ideal for storing root keys in an offline, secure device FIPS 140-3 Level 3 validated

Typical use cases
Root CAs
Proof of concepts

FIPS 140-3 Level 3 – Luna Network HSM, Luna PCIe HSM

First HSM in the industry to receive FIPS 140-3 Level 3 validation

Continuing our commitment to pioneering crypto advancements and delivering top-tier protection for our customers' most sensitive data

FIPS 140-3 more aligned to international standards, evolving requirements such as PQC and better suited to today's technologies

Key Details:

- The Luna Network and PCIe HSMs listed under "Luna K7 Cryptographic Module" (Certificate #4684)
- All the models in both the A and S series are validated
- All FIPS 140-2 certificates will be moved to the Historical List on Sept. 21, 2026

FIPS 140-3 Level 3 – Luna USB HSM

Luna USB HSM 7 receives FIPS 140-3 Level 3 validation

Continuing our commitment to pioneering crypto advancements and delivering top-tier protection for our customers' most sensitive data

FIPS 140-3 more aligned to international standards, evolving requirements such as PQC and better suited to today's technologies

Key Details:

- The Luna USB HSMs listed under "Luna G7 Cryptographic Module" (Certificate #4962)
- Includes Luna Backup HSM 7
- All FIPS 140-2 certificates will be moved to the Historical List on Sept. 21, 2026

Luna HSM Traditional Markets

- PKI
- Transaction Protection
- Identity Protection
- Software Supply Chain Protection
- Root of Trust For data security platforms

Luna HSMs establish a foundation of digital trust by generating, storing and protecting root keys for PKI, cloud, database encryption and the platforms used to secure them

Luna HSM Emerging Markets

Quantum-safe crypto agility

Implement quantum resistant algorithms within the HSM

Quantum safe keys

Digital assets

CBDC, blockchain, self-sovereign IDs

HSMs provide strong protection for NextGen financial asset products

Global Digital Identities

eIDAS 2.0 introduces self-sovereign identities (mobile wallets, etc.)

Protect issuance and verification of credentials (SSL an enabler of digital services for citizens)

5G / P5G

Protect subscriber identities

Protect network data

New algorithms (TUAK milenage)

Along with our broad partner ecosystem, Luna HSMs seamlessly form a root of trust for modern and future technologies

Transforming Global Finance: The Era of Digital Assets

"Cryptocurrency market cap hits **$3.2 trillion** in November 2024"

Stablecoins, cryptocurrencies, security tokens, tokenized real-world assets & CBDCs are now mainstream

$2.2 billion stolen in cryptocurrency hacks in 2024 up 21%

***Securing private keys** remains crucial for protecting digital assets*

Market Definition

What are Digital Assets?

Any type of digital or virtual item that has value, including cryptocurrencies, digital tokens, and non-fungible tokens (NFTs).

These assets are created, stored, and traded on a digital platform, such as a blockchain, and can be bought, sold, or traded like traditional assets.

Market Opportunity: Digital Assets Ecosystem and Network Touches over 1B+ Consumers

Banks & Custodians

- Custody
- Asset tokenization
- Treasury operations
- Stablecoin issuance

Asset Managers

- Fund tokenization
- Custody
- Distribution

Broker & Neobanks

- Crypto trading
- Yield products
- Payments
- Treasury operations

Payment Service Providers

- Stablecoin payments
- Digital accounts
- Treasury operations
- Loyalty programs

Market Makers & OTCs

- Trading & Settlement
- Treasury Operations
- Collateral Management

Exchanges

- Custody
- Treasury operations
- Collateral Management

Official Institutions

- CBDC Trials
- Permissioned DeFi
- On Chain FX
- Programmable Money

Enterprises

- Web3 experiences
- Loyalty programs
- Stablecoin payments

HSMs for Digital Assets: A Secure and Compliant Signing Solution

Featured Thales Technology Partners:

Fireblocks

Full Private Key Ownership

FIPS 140-3 L3 and Common Criteria certified root of trust for digital asset signing

Enable Faster Transactions

Flexible hot, warm, and cold signing workflows

Address Ongoing Regulations

Industry Regulations: MAS, HKSFC, PCI, FINMA, BaFin, MiCA

Compliance: GDPR, eIDAS

Digital transformation changing the Digital Identity industry

"Global Digital ID solution market projected to grow to $133.19B by 2030"

Government initiatives and regulations (CCPA, GDPR, eIDAS, HIPAA) supporting digital ID transformation

EU Digital eIDs & Wallets

eIDAS 2 regulation of remote qualified digital signatures for QTSPs

eIDAS 2 Compliant, Remote Qualified Signatures

Featured Thales Technology Partners:

ascertia nextsense

Enhanced Security

Protect the signing process against cyber threats & meet compliance with latest regulations

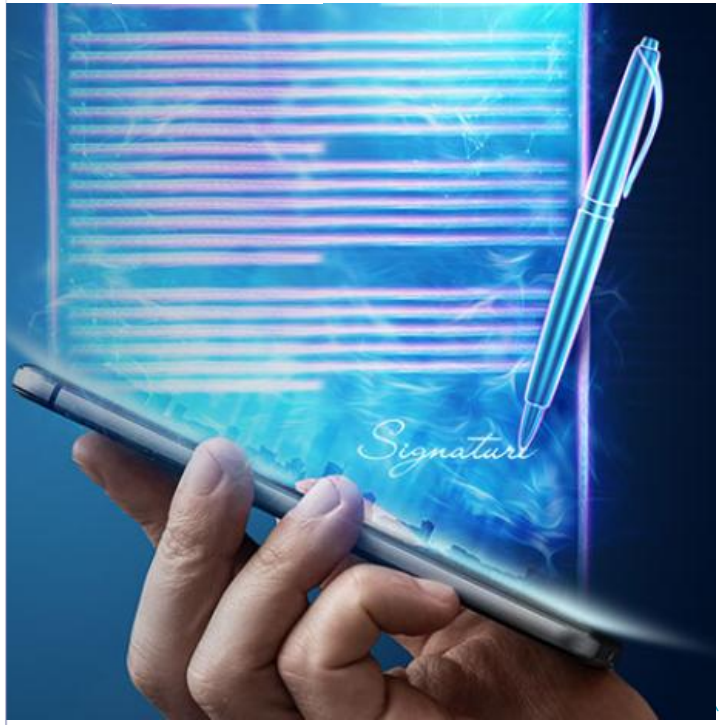
Qualified Digital Signatures

Ensure the authenticity, integrity and non-repudiation of digital signatures & seals

eIDAS 2 Compliant RQSCD

Common Criteria certified and meets PP:

- ✓ EN 419 221-5 (HSMs)
- ✓ EN 419-241-2 (SAM)



Luna HSM 5G Security Use Cases

> Protect subscriber privacy, identities and authentication

End-to-end security of 5G subscriber identifiers (SUCI de-concealment) & subscriber authentication

> Protect PKI, critical infrastructure and networks

Secure 5G VNFs & the entire PKI-based network and infrastructure with a FIPS 140-3 Level 3 HSM

Luna HSMs designed specifically for 5G

Proven UDM integration
Luna HSM has been validated by Ericsson and HPE, with other NEP integrations in progress

ERICSSON
Hewlett Packard Enterprise

Superior performance:
meets high throughput needs of telcos and max performance through multi-threads and high availability clusters
Low latency with fast response times

5G algorithms embedded:
Milenage, TUAK, COMP128, quantum resistance

Compliance and certifications:
Luna HSMs are certified to the highest standards including FIPS 140-2 Level 3 and Common criteria EAL 4+ certified

Follow 5G security best practices:
GMSA, 3GPP, ENISA all recommend using an HSM to protect network credentials and user privacy

GSMA 3GPP A GLOBAL INITIATIVE 5G enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

THE QUANTUM THREAT

Where are we at?

Gartner declares traditional cryptography will be unsafe by 2029

Gartner Insights Our Solutions Conferences

Begin Transitioning to Post-Quantum Cryptography Now

Quantum computing will render traditional cryptography unsafe by 2029. It's worth starting the post-quantum cryptography transition now.

By **Mark Horvath** | September 30, 2024

Crypto-Agility Timeline

2022 2023 2024 2025 2026 2027 2028 2029 2030

Current

- Build crypto-graphic metadata database
- Build crypto policies for next phases
- Lifeboat exercise for data (L/M/S term use)
- Plan transition phase plan
- Start crypto-agile dev strategy (e.g., CCOE)

Transition

- Implement transition plan
- Purge useless/expired data with weak crypto
- Implement transitional crypto policies
- Implement crypto-agile application development and move to production

Ongoing

- End of life nonagile applications
- Enforce strong crypto polices for data
- Vet and test new PQ algorithms
- Full transition to CCOE

Source: Gartner

Gartner

…but just in…..

IBM

IBM **Newsroom** News Media resources Inside IBM Blog

IBM Sets the Course to Build World's First Large-Scale, Fault-Tolerant Quantum Computer at New IBM Quantum Data Center

Jun 10, 2025

- IBM Quantum roadmap, processors, and infrastructure outline clear path to IBM Quantum Starling, expected to be first large-scale, fault-tolerant quantum computer
- Breakthrough research defines key elements for an efficient fault-tolerant architecture — charting the first viable path toward a system projected to run 20,000 times more operations than today's quantum computers
- Representing the computational state of IBM Starling would require the memory of more than a quindecillion (10^{48}) of the world's most powerful supercomputers

Regulatory bodies agree: Prepare now for Post-Quantum Cryptography

Prototyping post-quantum cryptography (PQC)

52%

Of respondents said PQC is their primary approach to address the future compromise of classical encryption techniques.

2024 Data Threat Report

2024 – PQC Implementation Becomes Reality

NIST
PKI Consortium
CAB CA/BROWSER FORUM
Accredited Standards Committee X9 Inc. Financial Industry Standards
ETSI World Class Standards
CSA cloud security alliance
CFDIR PQC Working Group
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
ANSI
IETF

Hybrid of classical cryptography and PQC

Crypto agile solutions

In 2024, NIST published the first PQC Standards – with other global standard bodies set to quickly adopt those as their own. Each of these bodies recommend beginning implementation immediately using solutions that are hybrid to start and crypto agile.

PKI Agile Certificates format

Pure Quantum

Serial number: xxxx
Issuer: Thales
Subject: MrTrust
Valid-From: mm/dd/yyyy
Valid-To: mm/dd/yyyy
Subject public key: PQC PubKey
Issuer Signature: PQC_Sign

Hybrid composite

Serial number: xxxx
Issuer: Thales
Subject: MrTrust
Valid-From: mm/dd/yyyy
Valid-To: mm/dd/yyyy
Subject public key: ASN1 Seq(**Classical PubKey**, **PQC PubKey**)
Issuer Signature: ASN1 Seq (**RSA_ECC_Sign**, **PQC Sign**)

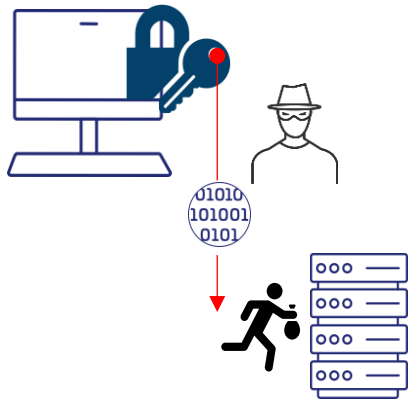
Hybrid extensions

Serial number: xxxx
Issuer: Thales
Subject: MrTrust
Valid-From: mm/dd/yyyy
Valid-To: mm/dd/yyyy
Subject public key: Classical PubKey
Issuer Signature: RSA_ECC_Sign

Extensions: PQC Pub Key
Extensions: PQC Sign

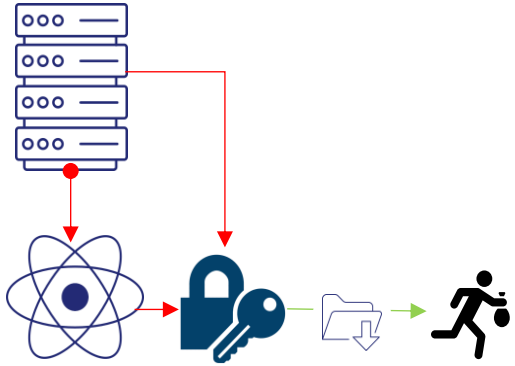
Harvest Now, Decrypt Later means data secured today is at risk now

Today – Harvest Now



Attacker steals your encrypted data and stores it in their server. Long life data is especially vulnerable.

Future – Decrypt Later



The attacker later uses quantum computers to decrypt the stolen data which can then be sold or traded on the black market.

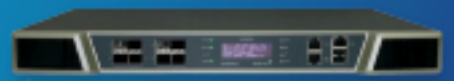
Cited harvest now, decrypt later attacks as their leading interest in PQC.

2024 Thales, Data Threat Report

Thales' Growing Quantum Partner Ecosystem

VERIFIED SOLUTION
THALES

Luna HSM



HSE (High Speed Encryptors)

CipherTrust Platform

A Collective Approach to Quantum Readiness

Work with your Technology Partners

Work with standard bodies

Sandbox Testing

Hybrid PQC in production

Luna HSM Firmware v7.9 Release: NIST-Approved PQC Algorithms Now Built-In

- Brings production-ready, NIST-approved PQC algorithms directly into the core of Luna HSMs
- Helps customers and partners to develop stable, standards-aligned solutions and seamlessly integrate quantum-safe cryptography into their systems and infrastructure, protecting critical applications, identities, transactions and sensitive data
- Ensures long-term protection against emerging quantum threats, including Harvest-Now, Decrypt-Later (HNDL) attacks

THE LUNA HSM ROADMAP

Where are we at?

Luna HSM Product Roadmap 2025

LMS/HSS

Key Rings & Clustering

ML-KEM / ML-DSA

FIPS 140-3 L3 Submission (Network &PCIe)

ML-KEM / ML-DSA Wrapping & Unwrapping

LMS/HSS large file signing

PQC Milestone

All Luna HSMs PQC-ready with native support for NIST-standardized PQC algos

FIPS 140-3 L3 Submission (USB)

JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

Q1 Q2 Q3 Q4

**Tentative. Dates and priorities subject to change.*

THALES
Building a future we can all trust

Contact

John Ray

Director – HSM Product Management

+1 613 614-9304

john.ray@thalesgroup.com

THALES

Building a future we can all trust

Thank you

cpl.thalesgroup.com