Solution Brief

THALES
CYBERSECURITY

Securing Digital Assets with Thales Luna HSMs

The hardware foundation of digital trust for rising risks and evolving regulatory demands

cpl.thalesgroup.com

THALES

CYBERSECURITY

What Are Digital Assets?

Digital assets are any form of value represented and transacted in a digital format, including cryptocurrencies and stablecoins used for payments and trading, as well as tokenized assets such as securities, deposits, or real-world assets. These assets are created, managed, and exchanged on distributed platforms like blockchains, forming the foundation of modern digital finance built on decentralization, programmable money, and digital ownership.

Introduction: Rapid Digital Asset Adoption and Growing Financial Risk

Digital assets have become a significant part of global finance. Stablecoins now handle more transactions by value than Visa and Mastercard combined, and international blockchain settlement volumes have exceeded six trillion dollars annually (Delphi Digital, 2025). Tokenization of real-world and financial assets on distributed ledger platforms is also gaining momentum, with institutional pilots expanding across capital markets, payments, and cross-border settlements (Bank for International Settlements, 2024). As a result, financial institutions across banking, payments, and capital markets are accelerating digital asset strategies to meet client demand and remain competitive in a rapidly evolving landscape.

This growth has increased the importance of strong security foundations. In 2025, losses from crypto-related hacks reached approximately $3.4 billion, reinforcing the need for robust key management and security controls as institutions scale digital asset operations. Even among centralized platforms with mature security programs, private keys remain a critical point of exposure. In the first quarter of 2025, centralized such as custodial exchanges and asset platforms accounted services accounted for 88% of all funds stolen, underscoring the importance of securing private key operations at the hardware level (Chainalysis, 2025).

As adoption continues to scale in value and complexity, financial institutions require a security architecture designed to protect private keys at the core. Trusted and proven Hardware Security Modules (HSMs) provide this foundation, delivering a reliable hardware-based root of trust for safeguarding keys and supporting the digital asset workflows built around them.

The Challenge: Security Gaps and Expanding Global Regulation

Even as digital asset initiatives accelerate, many institutions still struggle to implement the controls needed to operate securely at scale. Private keys must be generated, stored, and used in a way that prevents unauthorized access while supporting high-volume signing, multi-party approval workflows, and separation of duties. Software-based approaches to key storage are increasingly inadequate, especially as attackers focus on compromising private keys as a primary route to fraud and theft.

At the same time, regulatory expectations are becoming more demanding and more aligned across major financial centers. Frameworks such as Hong Kong SFC's Virtual Asset Trading Platform Guidelines, MAS notices in Singapore, MiCA in the European Union, BaFin guidelines in Germany, and FINMA requirements in Switzerland all place clear expectations on custody controls, key management, operational resilience, and auditability. Institutions must now demonstrate that their digital asset infrastructure can deliver consistent policy enforcement, verifiable key protection, and transparent governance across all deployment models.

Meeting these requirements calls for a trusted security foundation that protects private keys, controls transaction signing, and supports compliance without slowing innovation. Certified HSMs provide this foundation by securing critical operations within tamper-resistant hardware and delivering the assurance that regulators and institutional risk teams expect.

The Solution: Institutional-Grade Digital Asset Security Backed by Luna HSMs

Thales Luna HSMs protect digital assets by providing a hardware root of trust, ensuring private keys and signing operations are secured in certified, tamper-resistant hardware, delivered on-premises or as a service to suit modern digital asset platforms. They provide proven secure key generation and protect the private keys used in signing applications within customer-owned, FIPS validated hardware, ensuring that keys remain fully isolated from application layers, online systems, and cloud environments where most attacks originate.

By performing key creation, storage, and signing in tamper-resistant hardware, Luna HSMs strengthen a range of digital asset custody models. While many early digital asset platforms prioritized software-only simplicity, institutional clients and regulators now increasingly expect private keys to be secured by certified HSMs. Deployed on-premises or as a service and abstracted behind standard APIs, hardware-based security supports evolving custody architectures without becoming a constraint. Institutions gain a verifiable root of trust behind their software key management workflows, reducing single points of failure and ensuring that approvals, signing policies, and governance rules are enforced consistently. This approach provides the control and assurance required for institutional-grade digital asset operations.

Luna HSMs integrate with leading custody platforms, blockchain infrastructure, wallet technologies, and tokenization engines. Customers can deploy **Luna HSMs** on-premises, in the cloud, as a service, on the **Thales Data Protection on Demand (DPoD) cloud marketplace**, while maintaining consistent security, governance, and operational control. This flexibility to choose deployment models, combined with crypto-agile and quantum-ready security, provides institutions with a strong foundation to expand digital asset capabilities while reinforcing trust, performance, and regulatory alignment.

Luna HSM Deployment Models for Digital Assets

Flexible Luna HSM deployment options for digital assets in the cloud, on-premises or across hybrid environments:

Benefits:

Full key ownership and certified assurance: Keys are generated, stored, and used inside customer-owned, FIPS-validated, and Common Criteria certified Luna HSMs. Signing is performed within hardware built to the highest assurance levels. Luna HSMs have crypto agility built in, including support for NIST-standardized post-quantum algorithms, and the flexibility to adopt upcoming schemes.

Seamless integration with institutional environments: Luna HSMs integrate with regulated infrastructures and connect to custody platforms supporting diverse custody architectures, as well as blockchain systems, reducing operational friction for security, governance, and audit teams.

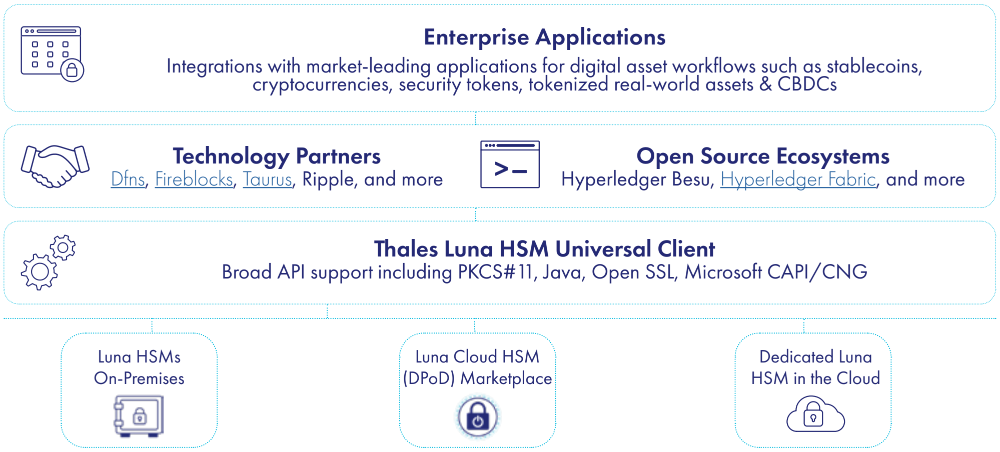
Support for hot, warm, and cold signing workflows: Institutions can run real-time online approvals or fully offline signing using controlled mechanisms. This flexibility supports diverse risk models and custody approaches.

Advanced governance and policy controls: Luna HSMs enforce granular controls, including multi-approval signing, address whitelisting, and transaction limits. Immutable logs support auditability and regulatory transparency.

Asset tokenization and smart contract support: Luna HSMs secure the on-chain lifecycle of tokenized assets and support signing for smart contract interactions, including stablecoins and real-world asset tokenization.

Connectivity across digital asset ecosystems: Luna HSMs integrate with on-ramps, off-ramps, liquidity providers, issuers, and settlement platforms while keeping private keys fully protected in hardware.

Built for global regulatory readiness: Luna HSMs support alignment with frameworks, including SFC, MAS, MiCA, BaFin, FINMA. Granular segregation of keys, tenants, and policies maps environments to specific business units, regions, and regulatory requirements.


Enterprise Applications
Integrations with market-leading applications for digital asset workflows such as stablecoins, cryptocurrencies, security tokens, tokenized real-world assets & CBDCs

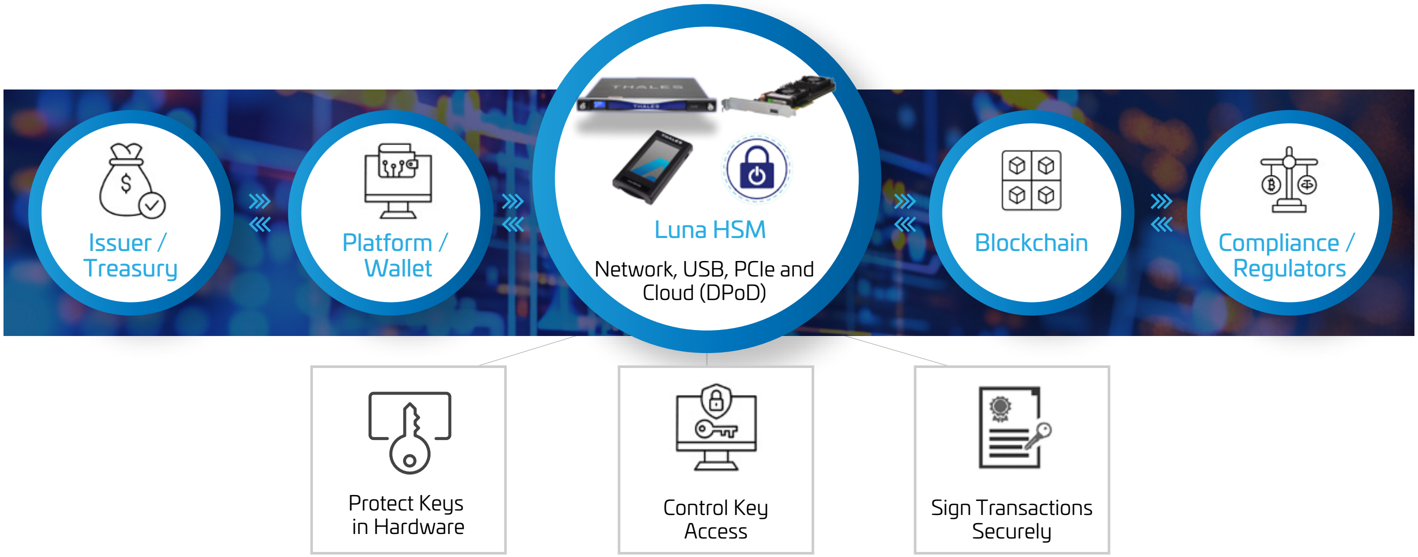
Technology Partners
Dfns, Fireblocks, Taurus, Ripple, and more

Open Source Ecosystems
Hyperledger Besu, Hyperledger Fabric, and more

Thales Luna HSM Universal Client
Broad API support including PKCS#11, Java, Open SSL, Microsoft CAPI/CNG

Luna HSMs On-Premises
Luna Cloud HSM (DPoD) Marketplace
Dedicated Luna HSM in the Cloud

Deployment models that bring Luna HSM security to digital asset environments.



Luna HSM provides a certified hardware root of trust for key generation, access control, and transaction signing across the digital asset ecosystem, available in multiple form factors.

Summary

As digital assets move into the core of institutional finance, the stakes for private key protection have never been higher, and key compromise remains one of the biggest drivers of financial loss across digital asset platforms. Thales Luna HSMs give institutions a trusted way to address this risk by performing key generation, protection, and transaction signing inside certified, customer-owned hardware. Keeping keys within FIPS-validated and Common Criteria certified HSMs strengthens security posture, supports regulatory expectations, and significantly reduces the risk of misuse or theft. Luna HSMs integrate with leading custody platforms, blockchain and tokenization platforms, and the broader digital asset ecosystem. Built on a crypto-agile, quantum-safe foundation and available across flexible deployment models, Luna HSMs provide the root of trust for digital asset adoption, helping institutions scale securely while demonstrating control to clients and regulators.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

Learn more about Luna HSMs

Free trial for Luna Cloud HSM for Hyperledger Fabric on DPoD

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us