

Banking-Grade Digital Asset Custody with Taurus and Thales

Hardware-Enforced
Governance and Key
Protection Using Taurus
and Thales HSMs

Key Outcomes

- **Hardware-rooted transaction control:** Keys, approvals, and governance policies are enforced inside certified Thales Hardware Security Modules (HSMs).
- **Bank-aligned digital asset security:** Digital asset operations use the same hardware trust models adopted in regulated financial environments.
- **Unified custody security:** A single hardened architecture supports hot, cold, and air-gapped deployments.
- **Regulatory-ready operations:** Enable custody, asset tokenization, and stablecoin services with audit-aligned controls.

The Challenge: Securing Digital Asset Governance

As financial institutions expand into digital asset custody, the security challenge is no longer just protecting private keys. It is ensuring that transaction governance itself cannot be bypassed.

Many digital asset platforms rely on software-based orchestration layers to validate approvals, roles, and policies before requesting a cryptographic signature. While these models may offer flexibility, they introduce a critical dependency: if the application layer is compromised, governance controls can fail, leading to unauthorized or irreversible transactions.

For banks and regulated institutions, this creates a gap between traditional financial security standards and digital asset infrastructure:

- Governance and approval policies may not be cryptographically enforced
- Transaction integrity may depend on software trust assumptions
- Security models may fall short of banking-grade standards

Institutions need a digital asset custody architecture that secures both keys and transaction governance at the hardware level, aligning digital asset operations with the security principles already applied to mission-critical financial systems.

The Solution: Hardware-Rooted Digital Asset Custody

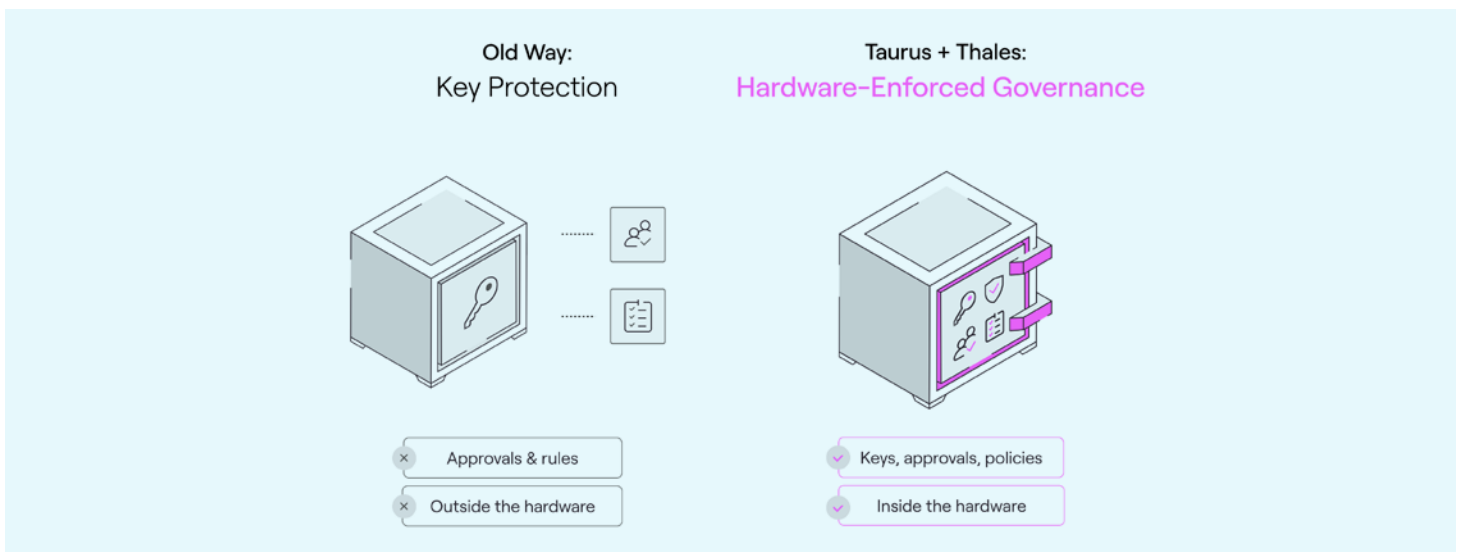
Taurus and Thales deliver a joint solution for banking-grade digital asset custody, designed to meet the security, governance, and regulatory expectations of financial institutions.

Taurus provides a regulated, enterprise-grade digital asset custody platform that enables institutions to operate custody, tokenization, and stablecoin services. Thales delivers the cryptographic foundation through Thales HSMs, establishing a certified hardware root of trust for digital asset operations.

By tightly integrating Taurus custody services with Thales HSMs, the solution ensures that critical security controls are enforced at the hardware boundary, rather than relying on software-only orchestration layers.

Together, Taurus and Thales enforce transaction governance and key protection at the hardware security boundary across all custody models.

This architecture aligns digital asset custody with the same security principles already trusted for mission-critical financial systems, enabling institutions to adopt digital assets with confidence, control, and regulatory alignment.



Why Hardware-Enforced Policy Matters

Digital asset security is not only about protecting private keys. It is about ensuring who can authorize a transaction, under what conditions, and how those rules are enforced.

When governance and approval logic live outside the cryptographic boundary, security depends on software controls and orchestration layers behaving exactly as intended. If those layers fail or are compromised, policies can be bypassed.

By enforcing transaction approvals and policies inside Thales HSMs, Taurus and Thales ensure governance is cryptographically bound to the signing operation itself. This approach aligns digital asset custody with established banking security principles, where critical controls are enforced at the hardware trust boundary rather than assumed in software. This approach reinforces a custody model in which governance is protected by hardware rather than assumed in software.

Features and Benefits

- **Secure Key Protection**

Private keys never leave the Thales HSMs. All cryptographic operations, including key derivation and transaction signing, are performed within certified hardware, reducing exposure to software-based attacks.

Benefit: Strong protection against key compromise and insider threats.

- **Hardware-Enforced Transaction Governance**

Transaction approvals and governance policies are cryptographically verified within Thales HSMs rather than relying on application-layer enforcement.

Benefit: Prevents unauthorized transactions, even in the event of application-layer compromise.

- **Client-Controlled Key Management**

Keys can be deployed on-premises or managed environments, with institutions retaining full control. Taurus never accesses private keys.

Benefit: Supports sovereignty, compliance, and internal security policies.

- **Flexible Custody Models**

Support hot, cold, and air-gapped custody models using a single security architecture.

Benefit: Align operational models with risk tolerance without changing security foundations.

- **Regulatory-Aligned Security Architecture**

The solution leverages FIPS-validated Thales HSMs and supports audited, high-assurance development practices.

Benefit: Simplifies alignment with regulatory requirements and internal risk management frameworks.

Use Cases: Securing Digital Asset Operations at Scale

The Taurus and Thales solution supports a range of digital asset use cases while maintaining consistent, banking-grade security controls across all deployment models.

Cryptocurrency Custody

Enable secure custody of digital assets across multiple blockchain networks, with private keys and transaction approvals protected inside certified hardware. Institutions can scale custody operations while maintaining strong governance and control over asset movement.

Tokenized Financial Instruments and Real-World Assets

Support the issuance and custody of tokenized securities and real-world assets with transaction rules and approvals enforced at the hardware level. This enables regulated workflows, such as transfer restrictions, regulatory holds, and corporate actions, without relying solely on software-based logic.

Stablecoin Custody and Issuance

Secure both the custody of reserves and the authorization of mint and burn operations using hardware-enforced approval policies. This ensures stablecoin operations meet governance and control expectations aligned with regulated financial environments.

Across all use cases, institutions apply the same banking-grade security controls while adapting operational models to business needs.

Taurus Digital Asset Custody Platform

Taurus provides a regulated, enterprise-grade platform for securing and operating digital asset services. Designed for financial institutions, Taurus enables custody, tokenization, and stablecoin operations while aligning with banking and regulatory expectations.

At the core of the platform is a custody model that prioritizes control, governance, and risk management. Taurus integrates with Thales HSMs to support strong custody governance and operational control aligned with banking expectations.

Key Taurus capabilities include:

- **Enterprise-grade digital asset custody**
Secure operation across hot, cold, and air-gapped environments.
- **Built-in transaction governance**
Cryptographic validation of approvals, roles, and authorization policies.
- **Client-controlled operations**
Institutional control over keys and custody policies.
- **Support for regulated digital asset use cases**
Custody, tokenization, and stablecoin operations within a consistent security framework.

The Taurus Way: Hardware-Enforced Governance

Taurus leverages Thales Luna and ProtectServer HSMs as the hardware root of trust for digital asset custody, ensuring private keys are generated and used exclusively inside certified hardware.

Through a proprietary Functionality Module, [Taurus-PROTECT](#) solution extends the HSM trust boundary to include transaction governance logic, enabling multi-party approvals, policy validation, and role-based access controls to be cryptographically verified inside the HSM before any transaction is authorized. Key material is protected throughout its lifecycle, with signing keys derived on demand and securely erased after use.

Supported by audited build processes and independent verification, this architecture enforces governance at the hardware level, aligning digital asset operations with the security and assurance expectations of regulated financial institutions.

Thales HSMs - The Foundation of Digital Trust

Thales Luna HSMs

[Thales Luna HSMs](#) provide a trusted hardware foundation for securing cryptographic keys used in digital asset custody and transaction processing environments. Backed by independently validated security, including FIPS 140-3 Level 3 and Common Criteria EAL4+, Luna HSMs help institutions meet regulated custody requirements for governance, separation of duties, and audit readiness.

With more than 30 years of HSM expertise, Thales is trusted by leading financial institutions worldwide to protect cryptographic keys in environments where confidentiality, integrity, and availability are critical. Luna HSMs integrate with the Taurus platform to secure private key generation and transaction signing inside tamper-resistant hardware, while enabling long-term crypto-agility and post-quantum readiness through native support for NIST-standardized PQC algorithms directly within the HSM firmware.

Thales ProtectServer HSMs

Within the Taurus solution, [ProtectServer HSMs](#) support secure transaction signing and hardware-enforced policy execution at scale. FIPS 140-2 Level 3 validated, ProtectServer HSMs are widely deployed across payments, identity, and core financial systems.

Summary

Taurus and Thales provide a secure, compliant foundation for digital asset custody, designed for financial institutions that require banking-grade controls.

By protecting private keys, transaction approvals, and governance policies inside Thales HSMs, the joint solution enables institutions to operate digital asset services with confidence, flexibility, and regulatory alignment.

As digital assets mature, Taurus and Thales help institutions secure what matters most: trust, control, and long-term confidence.

About Taurus

Founded in 2018, Taurus is a Switzerland-based financial technology company providing enterprise-grade digital asset infrastructure, with 13 offices around the world. It offers services for issuing, storing, and trading all types of digital assets, including cryptocurrencies, tokenized assets, stablecoins, and digital currencies. Taurus has earned global recognition for excellence in digital asset infrastructure, receiving eight industry awards in 2025, including Euromoney's World's Best Custody Services, Digital Banker's Best Digital Assets Solution by a Vendor, and Future of Finance's Best Digital Asset Tokenization Platform. Additionally, Taurus operates a marketplace for private assets and tokenized securities and is a securities firm regulated and supervised by FINMA. For more information, visit www.taurushq.com

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.