Solution Brief

THALES
CYBERSECURITY

Dfns

Securing Digital Asset Operations

Dfns Wallet-as-a-Service Platform and Thales Luna HSM

cpl.thalesgroup.com

THALES
CYBERSECURITY

Dfns

Key Outcomes

- Unified multichain wallet operations across users, assets, and transactions from one secure interface
- Private keys used for transaction signing always remain protected with customer-owned and managed Luna HSMs, complying with audit and regulatory mandates
- Compliance alignment with MiCA, DORA, GENIUS, GDPR, HKMA, and residency mandates
- Automated governance, approvals, and access control
- High-performance, scalable transaction processing and orchestration
- SaaS, hybrid, and on-premises options—with SOC 2 Type II + ISO 27001/17/18–certified SaaS

Barriers to Secure Digital Asset Growth

Financial services institutions (FSIs) are quickly expanding into digital assets, including custody, payments, trading, tokenization, and settlement. However, as their operations grow, they face fragmented blockchain tools, complex workflows, and increasing regulatory pressures under MiCA, DORA, and GENIUS. Engineering teams need to deliver new products rapidly while managing risks like key compromise, misconfigured signing processes, limited audit trails, and inconsistent access controls. To innovate safely, organizations require a unified, high-security environment that simplifies development, reduces operational risks, and complies with evolving standards. Together, Dfns and Thales offer the secure, compliant foundation FSIs need to overcome these challenges.

Unified Digital Asset Security Architecture

Dfns and Thales deliver a combined architecture that anchors digital asset operations in certified hardware security while providing a programmable, API-driven orchestration layer for wallets, policies, and approvals.

Dfns and Thales combine a programmable Wallet-as-a-Service (WaaS) platform with industry-leading hardware security to provide a secure environment for digital asset management. Thales Luna Hardware Security Module (HSM) creates a tamper-resistant, FIPS-validated trust boundary for cryptographic key generation, storage, and signing. Keys never leave secure hardware, supporting global regulatory requirements and enabling BYOK, on-premises, and hybrid deployments for data sovereignty.

The Dfns platform enhances the Luna HSM hardware foundation with an API-first orchestration layer that manages wallet provisioning, user and device enrollment, policies, approvals, MPC/Luna HSM-based signing, monitoring, and audit logging. All objects and workflows, such as wallets, users, transactions, and signatures, are managed through a consistent interface.

Together, the integrated solution enables FSIs to generate, store, and orchestrate keys within Luna HSMs while utilizing Dfns to enforce governance, access controls, and transaction policies end-to-end. The result is a unified operating environment that enhances security, speeds up development, and supports always-on operations for custody, payments, tokenization, and more.

Dfns Platform Overview

Dfns WaaS helps FSIs optimize digital-asset operations and develop on-chain applications at scale. Its programmable wallet infrastructure consolidates lifecycle management, workflow governance, key orchestration, and integrations into a secure, unified operating system for blockchains, supporting custody, payments, trading, tokenization, and settlement.

The platform offers:

- **A unified operating system for** blockchains to manage wallets, users, policies, and transactions.
- **An API-first architecture** to automate workflows and embed wallets into applications, as every object and capability is programmatically exposed.
- **Zero-trust security** with Luna HSM-based key management, PKI controls, granular IAM, and hardware-backed authentication, so no single actor can move assets.
- **High performance** with sub-second signing and geo-redundant uptime.
- **Flexible deployment options** across SaaS, hybrid, or on-premises environments, aligned with MiCA/DORA, GENIUS, and GDPR.

Thales Luna HSM Overview

Thales Luna HSMs serve as the FIPS 140-validated hardware root of trust for digital asset security, generating and protecting cryptographic keys within a customer-owned, certified, tamper-resistant appliance. Keys never leave the Luna HSM, and all signing operations take place within secure hardware. Thales Luna HSMs can be deployed on-premises, in the cloud, as a service (available on Thales Data Protection on Demand), or across multiple environments to create a purpose-built hybrid HSM solution. Customers can maintain residency control while delivering the performance and availability needed for regulated financial operations.

Solution Key Features & Benefits

Unified Multichain Operations
Manage wallets, assets, and policies across supported blockchains through a single API, reducing fragmentation and simplifying expansion for supporting new assets and blockchains.

Hardware-Backed Security & Governance
Thales Luna HSMs anchor key generation, protection, access control, and signing inside customer-owned hardware, providing a trusted foundation for digital asset operations. Dfns enforces policies, approvals, thresholds, and granular IAM for regulated separation of duties.

Programmable Transaction Workflows
Automate approvals, treasury functions, settlement flows, and on-chain business logic using Dfns' orchestration layer integrated with Thales Luna HSM cryptographic operations.

Regulatory Alignment & Data Residency
Meet MiCA/DORA, GENIUS, and data-sovereignty requirements through BYOK, hybrid, and on-premises deployments, combined with Dfns' compliance-ready architecture.

High-Performance Continuity
Achieve sub-second signing, high throughput, and geo-redundant availability for mission-critical financial operations.

Dfns governs digital-asset workflows, while Thales Luna HSM provides the hardware root of trust for secure signing before blockchain execution

Accelerating Secure Digital Asset Innovation

Dfns and Thales provide a unified, secure, and programmable platform for digital-asset operations, ensuring full customer sovereignty over cryptographic keys. By anchoring key generation and signing inside Thales Luna HSMs, keys remain completely outside the WaaS layer and outside cloud-provider control, preventing exposure to jurisdictional access or third-party management.

Paired with Dfns' API-first orchestration, FSIs gain strong cryptographic control, automated governance, multichain scalability, and compliance-ready infrastructure. Together, Thales and Dfns help FSIs innovate faster, reduce operational risk, and confidently scale digital-asset services without compromising sovereignty, data security, or compliance.

About Dfns

Dfns is a leading Wallet-as-a-Service platform that provides secure, programmable infrastructure for managing digital assets and building onchain applications. Over 300 fintechs and institutions globally use Dfns to orchestrate wallet creation, key management, transaction workflows, onchain governance, and multichain integrations across a unified operating system.

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.

cpl.thalesgroup.com

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