

# Trusting Your Data Security: DataChain Private Blockchain with Thales Luna HSMs



Trust is the essential element in every human transaction, but by every metric, trust in existing systems and the security of the data enabling those systems is declining. The opportunity, technology, and partnerships exist to restore trust in data security and information exchange leveraging blockchain technology, strong authentication, and cryptographic key vaulting.

## The Solution: DataChain and Thales Luna HSMs Integration

Integrated with the DataChain private blockchain platform, Luna HSMs provide the logical and physical protection of the private keys used in combination with the distributed ledger for data security and sharing. Thales Luna HSMs generate, manage and store encryption keys and certificates in a certified root of trust across on premises, cloud and hybrid environments, ensuring they cannot be compromised.

Within a permissioned blockchain, transactions are validated and processed by participants that are already recognized by the ledger. This strengthens the security, increasing confidence for participants within the DataChain platform.

## Thales Luna HSMs

Thales Luna HSMs are robust, high-availability, and high-performance network appliances that store cryptographic materials (e.g., certificates, encryption keys, etc.) in a secure FIPS 140-2 Level 3 tamper-resistant hardware appliance. Storing these materials in hardware keeps them out of harm's way and ensures that only authorized administrators have access to important encryption keys.

A single Luna HSM can manage keys and accelerate operations to significantly improve the reliability, security, and scale of encryption performance. With Luna HSMs as a security infrastructure's trusted root, administrators can ensure the integrity of their cryptographic operations and adds the assurance that the critical private keys and digital identities are always secure regardless of environment.

### Thales Luna Cloud HSM Service on Data Protection on Demand (DPoD)

The Luna Cloud HSM on DPoD stores the private keys used by DataChain blockchain members to sign all transactions, and ensures cryptographic keys cannot be used by unauthorized devices or people for a range of blockchain applications. Luna Cloud HSM provides high assurance security in data centers and the cloud, enabling multi-tenancy of blockchain identities per partition as proof of transaction and for auditing requirements.

## Key Benefits

### High-Performance Processing

Luna HSMs offer market-leading performance and best-in-class processing speeds. High processing speeds allow administrators to offload cryptographic functions to improve server performance.

## Robust Security that Meets Compliance Standards

Luna HSMs offer the highest level of tamper-resistant security and are validated to be compliant with FIPS 140-2 Level 3 and Common Criteria EAL 4+ standards.

## Next-Generation Data Security

The DataChain platform stores, process, and encrypts keys in Luna HSMs. Luna HSMs are separate from the DataChain platform and provide the strongest cryptographic algorithms and hardware key management to guard digital identities.

## Multi-Level Access Control

Luna HSMs offer partitioning for signing/key management. Remote backup features allow administrators to securely move copies of their sensitive cryptographic material to the Luna Backup HSM.

## Key Features

### Robust security

Luna HSMs safeguard the private keys and associated certificates used by the DataChain platform to authenticate access. Luna HSMs serve as a root of trust to ensure the integrity of all blockchain cryptographic operations. The private key essential to each nodes operation never leaves the hardware appliance, making it impossible for unauthorized users to steal the keys needed to decrypt secured traffic or masquerade as network servers. The appliance's tamper-resistant design also provides significant physical security in addition to the logical security protecting the keys. This eliminates one of the biggest vulnerabilities in blockchains.

## Centralized Management and Operations

DataChain allows for a range of management options from individual to device/group-based management using a web interface. DataChain centralizes policy, reporting, visibility, and logging features to reduce management overhead while Luna HSMs can be clustered into high-availability configurations that can be managed as one unit. In addition, Luna HSMs can perform multiple operations—such as key generation, export, and root functions— where enterprises would normally require multiple appliances or solutions to manage the PKI infrastructure.

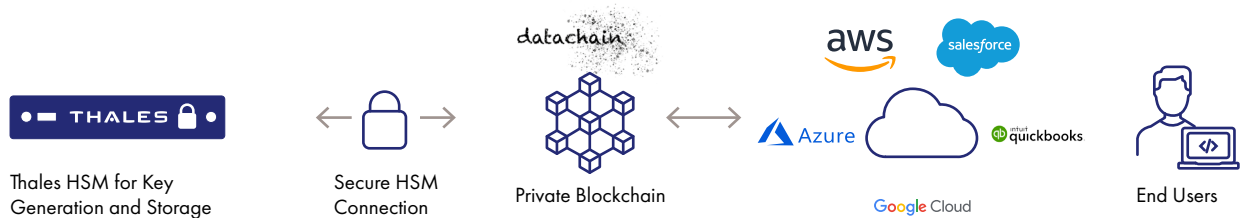
## Logging and auditability features

Luna HSMs combine proven hardware key management with rigorous logging features to provide indisputable audit records of access and cryptographic key usage. Separated administrative roles and flexible security policy management allows security teams to maintain tight control over the management of cryptographic keys. Knowing who is accessing the blockchain's private keys and being able to easily demonstrate detailed log records makes reporting for audits easier on security teams.

## Partition to Easily Scale

Luna HSMs can be separated into up to one hundred cryptographically isolated partitions, with each partition acting as if it were an independent HSM. Partitions provide a tremendous amount of scalability and flexibility, as a single HSM can act as the root of trust that protects the cryptographic key lifecycle of thousands of DataChain private blockchain nodes.

What's more, the partitions are designed to protect key material from other tenants on the appliance, meaning different lines of business can leverage the same appliance without fear of losing their keys to other tenants.



## Conclusion

Thales and DataChain work together to enhance data security and exchange so businesses can build the trust that drives their success. DataChain reduces the vulnerabilities of centralized databases while improving information sharing across business ecosystems. Luna HSMs support these efforts by ensuring that all cryptographic operations occur within a trusted infrastructure.

## About Thales





The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the

moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments

## About DataChain

The DataChain mission is to restore trust and confidence in the security and exchange of information. Utilizing private blockchain technology, DataChain combines world-class data protection and sharing capabilities to reduce cyber security risk and improve collaboration. Talk to us at: [datachain.world](https://datachain.world)

> [cpl.thalesgroup.com](https://cpl.thalesgroup.com) <    

**Contact us** – For all office locations and contact information, please visit [cpl.thalesgroup.com/contact-us](https://cpl.thalesgroup.com/contact-us)