

DATASHEET

nShield Multi-Tenancy

True isolation of cryptographic environments on shared HSM infrastructure

OVERVIEW

nShield Multi-Tenancy enables multiple tenants to operate in fully isolated cryptographic environments on shared nShield HSM infrastructure. Each tenant runs within its own independent security domain, with exclusive control of cryptographic keys, policies, and administration. Neither the HSM operator nor other tenants can access a tenant's cryptographic environment. The result is true separation of security domains, delivering the security assurances of dedicated HSMs with the efficiency, scalability, and flexibility of a shared platform.

Key Value at a Glance True tenant isolation

Each tenant operates in a dedicated cryptographic environment with no cross-tenant access.

Independent control

Tenants maintain exclusive ownership of keys, policies, and administrative authority.

Operational efficiency

Shared HSM infrastructure reduces hardware footprint, datacenter space, power, and cooling costs.

Compliance flexibility

Supports tenants with different regulatory and certification requirements on the same physical platform.



Why nShield Multi-Tenancy

Isolate, don't share.

nShield Multi-Tenancy is designed to isolate cryptographic environments, not merely partition resources. Each tenant is protected by strong, enforced boundaries that eliminate cross-tenant access and remove the need for tenants to trust one another, or the HSM operator, with their cryptographic assets. Each tenant has its own performance rates, to guarantee SLA and avoid service disruptions. Each tenant has its own performance rates, to guarantee SLA and avoid service disruptions.

HIGHLIGHTS

Core Capabilities

True Separation of Security Domains

Each tenant operates in a fully isolated cryptographic environment, providing the same security assurances as a dedicated HSM. Cryptographic operations, keys, and policies are strictly confined to tenant boundaries.

No Cross-Tenant or Provider Access

Tenant cryptographic environments are inaccessible to other tenants and to the Service Provider. This eliminates shared trust assumptions and significantly reduces risk exposure.

Independent Tenant Administration

Tenants manage their own cryptographic policies and operations through dedicated administrative access, enabling clear separation of responsibilities and governance.

Multi-Tenant Flexibility

Organizations can support multiple tenants per customer or application, enabling segmentation by environment, business unit, region, or workload sensitivity.

Optimization and Cost Efficiency

nShield Multi-Tenancy reduces the physical infrastructure required to support multiple cryptographic environments.

Performance

Tenants can be executed with separate performance rates to guarantee SLA or with dynamic performance scaling to optimize hardware usage.

Benefits Include

Reduced hardware requirements for HSM clusters, optimized datacenter footprint, lower energy consumption, and simplified operational management.

Multi-Compliance Support

Different tenants can operate with different certified firmware versions in isolated environments. This enables alignment with varying regulatory, regional, or industry compliance requirements without deploying separate physical HSMs.

Typical Use Cases

Service providers delivering isolated cryptographic environments to multiple customers, enterprises separating cryptographic control across development, test, and production environments, organizations segmenting cryptographic domains by business unit, geography, or application, regulated tenants requiring distinct compliance postures on shared infrastructure.

Key Benefits Summary

True isolation of cryptographic environments, no provider or cross-tenant access, independent tenant control, reduced hardware and operational costs, support for multiple compliance requirements, flexible and scalable deployment model.

