DATASHEET

nShield Multi-Tenancy

Strong 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 strong 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 Strong 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.

ENTRUST
SECURING A WORLD IN MOTION

HIGHLIGHTS

Core Capabilities

Strong 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 providing:

- A separate root of trust
- A dedicated cryptographic execution environment
- Its own instance of HSM firmware
- Independent key storage and Security World data

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.

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
Strong 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.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION