WHITE PAPER

nShield Multi-Tenancy

ENTRUST
SECURING A WORLD IN MOTION

Contents

Executive Summary

Organizations are under pressure to scale cryptographic services while maintaining strict security, compliance, and operational controls. As applications, business units, development environments, and external customers increasingly require dedicated cryptographic domains, traditional HSM deployment models often force tradeoffs between isolation, infrastructure costs, and operational complexity.

Entrust nShield® Multi-Tenancy addresses this challenge by enabling multiple cryptographically isolated environments to operate on a single nShield 5s HSM. Each tenant is assigned a dedicated Versatile Crypto Module (VCM), an isolated, containerized HSM instance within a physical nShield HSM. Each VCM contains its own Security World, firmware instance, key storage, policies, credentials, administrative controls, and endpoint connectivity. This architecture allows organizations to consolidate HSM infrastructure without compromising cryptographic separation.

Unlike traditional partition-based approaches that operate within a shared HSM firmware and administrative domain, nShield Multi-Tenancy establishes independent trust domains for each tenant. Infrastructure operators manage the physical HSM platform, while tenants maintain exclusive ownership and control of their cryptographic assets and policies. This separation reduces operational trust dependencies and minimizes the risk of cross-tenant exposure.

Key benefits include:

- **Strong cryptographic isolation** between applications, business units, customers, and environments
- **Reduced infrastructure costs** through HSM consolidation
- **Independent Security Worlds** and administrative control per tenant
- **Simplified operational management** and lifecycle administration
- **Support for diverse compliance requirements** within shared infrastructure
- **Flexible deployment models** for production, development, testing, disaster recovery, and remote data center environments
- **Controlled resource allocation across tenants** to help ensure consistent service levels and operational continuity

This white paper explains the architecture, isolation model, operational framework, trust assumptions, and deployment considerations behind nShield Multi-Tenancy, demonstrating how organizations can achieve scalable cryptographic operations while preserving security boundaries traditionally associated with dedicated HSM deployments.

Introduction

Modern organizations rely on cryptography to secure applications, protect sensitive data, and meet growing regulatory demands. As digital services scale, so does the need to support multiple applications, business units, and customer environments with distinct security, compliance, and operational requirements.

Entrust nShield® Hardware Security Modules (HSMs) provide a trusted foundation for secure cryptographic processing, key protection, and centralized key management. Built on the proven Security World architecture, they enable strong cryptographic separation and control across distributed environments.

nShield Multi-Tenancy extends this foundation by enabling multiple cryptographically isolated environments to run securely on a single HSM platform. Each tenant operates within its own independent cryptographic boundary, aiming to provide the assurance of dedicated infrastructure while improving scalability, flexibility, and resource efficiency.

Entrust has introduced multi-tenancy with its initial release on the embedded PCIe form factor, nShield 5s HSM. This white paper focuses on how multi-tenancy is implemented on the nShield 5s, with support for additional nShield models planned for a future release.

The Challenge: Scaling Cryptographic Infrastructure Without Compromise

As organizations expand digital services, adopt cloud delivery models, and support increasingly distributed environments, the demand for cryptographic protection continues to grow. Applications, business units, and external customers all require secure key management and cryptographic services – often with distinct security, compliance, and operational requirements.

Traditional approaches to deploying cryptographic infrastructure struggle to keep pace with these demands, creating a set of common challenges:

- **Balancing isolation and efficiency**

  Organizations must ensure strong separation between applications, environments, and customers, while avoiding unnecessary duplication of infrastructure.

- **Rising infrastructure and operational costs**

  Scaling cryptographic environments often requires additional hardware, increased data center footprint, and higher power, cooling, and management overhead.

- **Operational complexity at scale**

  Managing multiple cryptographic environments across distributed locations introduces administrative burden, increases the risk of misconfiguration, and complicates lifecycle management.

- **Inefficient use of resources**

  Fixed infrastructure allocations can result in underutilized capacity in some areas, while others require rapid scaling to meet demand.

- **Evolving compliance and regulatory demands**

  Organizations must support different security policies, certification requirements, and audit boundaries across environments – often within the same infrastructure footprint.

These challenges force organizations into difficult trade-offs between **security, cost, and operational efficiency**, limiting their ability to scale cryptographic services in a flexible and sustainable way.

The Solution: Multi-Tenant HSM Architecture

nShield Multi-Tenancy is designed to address this trade-off by enabling multiple, isolated cryptographic environments – each with its own keys, policies, and administrative control – to coexist on a single physical HSM.

This approach allows organizations to:

- Maintain **strong cryptographic isolation** between applications, business units, or customers
- **Reduce hardware footprint and cost** through consolidation
- Improve **operational efficiency** by simplifying infrastructure management
- Enable **flexible, scalable deployment models** aligned to workload demand

Core Concepts and Terminology

Understanding nShield Multi-Tenancy requires a clear distinction between a small number of core architectural concepts. The following definitions establish a common foundation for how multi-tenant environments are structured, isolated, and managed.

Component	Purpose
Security World	Fundamental cryptographic trust boundary within an nShield HSM environment.
Versatile Crypto Module (VCM)	An isolated, containerized HSM instance running within a physical nShield HSM.
Tenant	An independent entity – such as a group of applications, business unit, or external customer - that uses HSM services to perform cryptographic operations in an isolated domain.
Service Provider	The entity responsible for owning and operating the physical HSM infrastructure.
Platform Services	Set of operational functions required to manage the underlying HSM infrastructure.

These terms are used throughout this paper to distinguish between infrastructure control, tenant ownership, and the cryptographic boundaries enforced by nShield Multi-Tenancy.

Key Concepts in Multi-Tenant Operation

In a multi-tenant HSM architecture:

- **Isolation is enforced at the VCM level**

  Each tenant operates within an independent VCM, with no shared key material or administrative control.
- **Security Worlds remain the unit of cryptographic trust**

  Each tenant defines and manages its own Security World within its VCM.
- **Hardware is shared, but trust boundaries are not**

  While physical resources are shared, cryptographic environments remain fully independent.

By clearly separating **infrastructure control (service provider)** from **cryptographic ownership (tenant)**, and by enforcing isolation through **independent VCMs**, nShield Multi-Tenancy enables organizations to securely share HSM infrastructure without weakening established trust boundaries.

Established Foundations: Security World and Cryptographic Separation

Within the nShield HSM architecture, strong separation of cryptographic environments has long been enforced through the Security World framework. This longstanding model establishes clear trust boundaries that define how cryptographic keys are created, protected, and used, ensuring that key material and associated policies remain isolated – even when hosted on shared physical hardware.

The existing Security World architecture is fully compatible with multi-tenancy, offering the same key protection mechanisms.

This long-established, proven approach has enabled organizations to securely consolidate cryptographic workloads while maintaining strong isolation, operational independence, and compliance with regulatory requirements. nShield Multi-Tenancy builds on these established principles by extending isolation beyond a single cryptographic environment – enabling multiple, tenant-administered Security Worlds to coexist within a single HSM platform.

Learn more about Entrust Security World architecture **here**.

nShield 5s Architecture

To understand how Entrust nShield 5s HSMs support strong isolation models, it is helpful to first examine how the nShield 5s is structured. The nShield 5s uses a service-based architecture. Its services are separated into containerized management functions alongside the containerized VCM services of ncoreapi and CodeSafe 5.

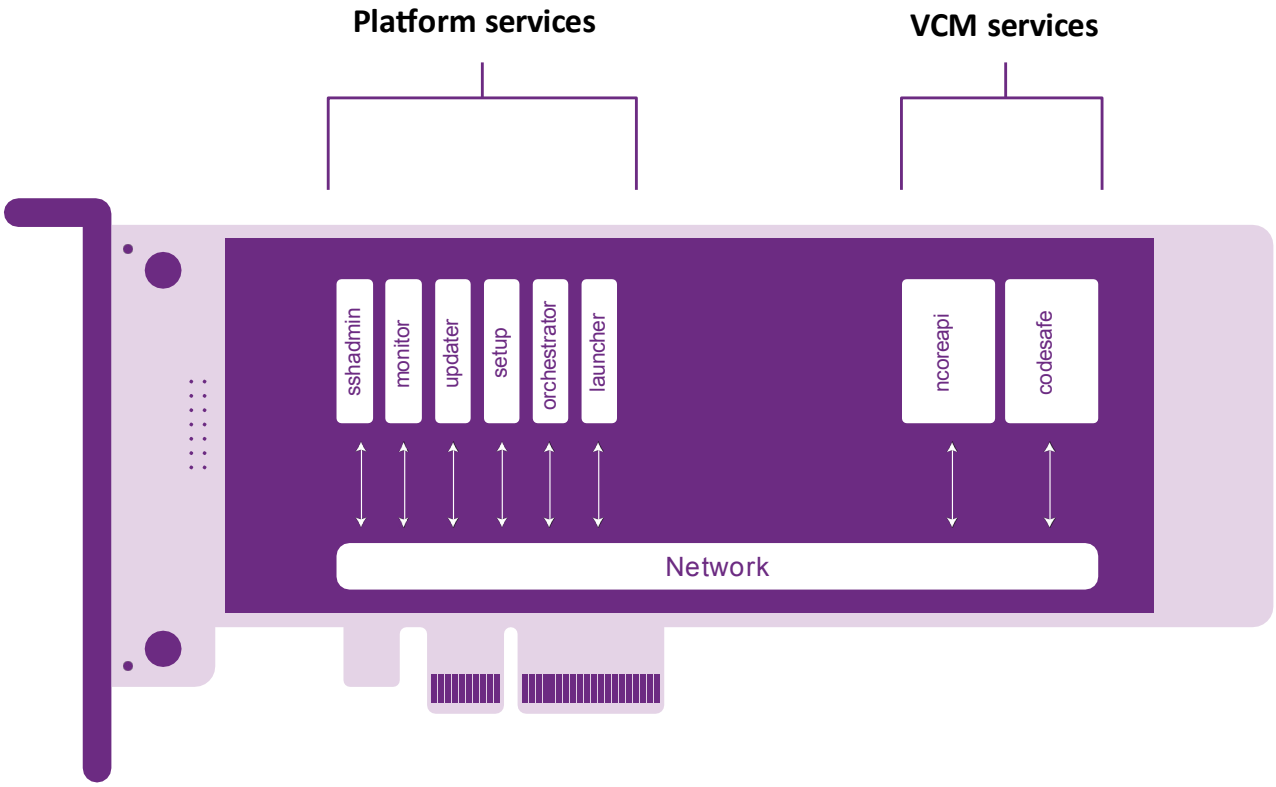


Figure 1: Illustration of the platform and VCM services in the nShield architecture

Unlike earlier nShield HSM firmware, the multi-tenant nShield 5s firmware presents to the host as a network-attached device. Its driver carries network traffic over the PCIe interface, effectively linking the host and HSM TCP/IP stacks.

Network connectivity and service access

- The HSM is assigned a link-local IPv6 address.
- Multiple SSH servers listen on different ports.
- Each port provides access to a specific service and its related command set, described below.

Service Name	Function	Host-side Client
sshadmin	Configures SSH credentials for other services	hsmadmin
updater	Firmware upgrades	hsmadmin
setup	Set/adjust time; request factory state	hsmadmin
monitor	Retrieve/manage system logs and statistics	hsmadmin
ncoreapi	Cryptographic operations	Security World tools and applications (via hardserver)

Each service has its own SSH client key pair for authenticating the corresponding host-side client. Although the hsmadmin tool can communicate with multiple services, it uses a different client key for each one. This allows host OS permissions to enforce service-level access control. For example, an automated monitoring process can be granted access only to the monitor service, while being denied permission to update firmware or perform cryptographic operations.

The ncoreapi service

The ncoreapi service provides the HSM's core functionality: generating, protecting, and using cryptographic key material.

The ncoreapi service is used exclusively by the nShield HSM client software, comprising:

- **The hardserver process**, which mediates access by multiple clients to one HSM, and from each client to potentially many HSMs
- **Security World administration tools** (new-world, createocs, generatekey etc.) to allow key protection to be configured
- **A number of API libraries** (PKCS#11, JCE, CAPI) to allow standard APIs for integration with standard applications.

The same software stack supports all HSMs in the nShield family, which all implement the nCore API command set.

Security World architecture

The Security World key management paradigm employs the following data stored securely within the HSM:

- A secret key shared between all HSMs in the Security World
- [A hash of] the root key, which is the root of trust used to authorize privileged operations within the Security World (such as recovering key material)
- Control and mode flags, relating to the Security World (for instance "FIPS 140 Level-3 mode," or whether audit logging is enabled)

This data is created or reloaded using the new-world tool (in conjunction with the Administrator Card Set).

None of the other services depend on this data for their functionality.

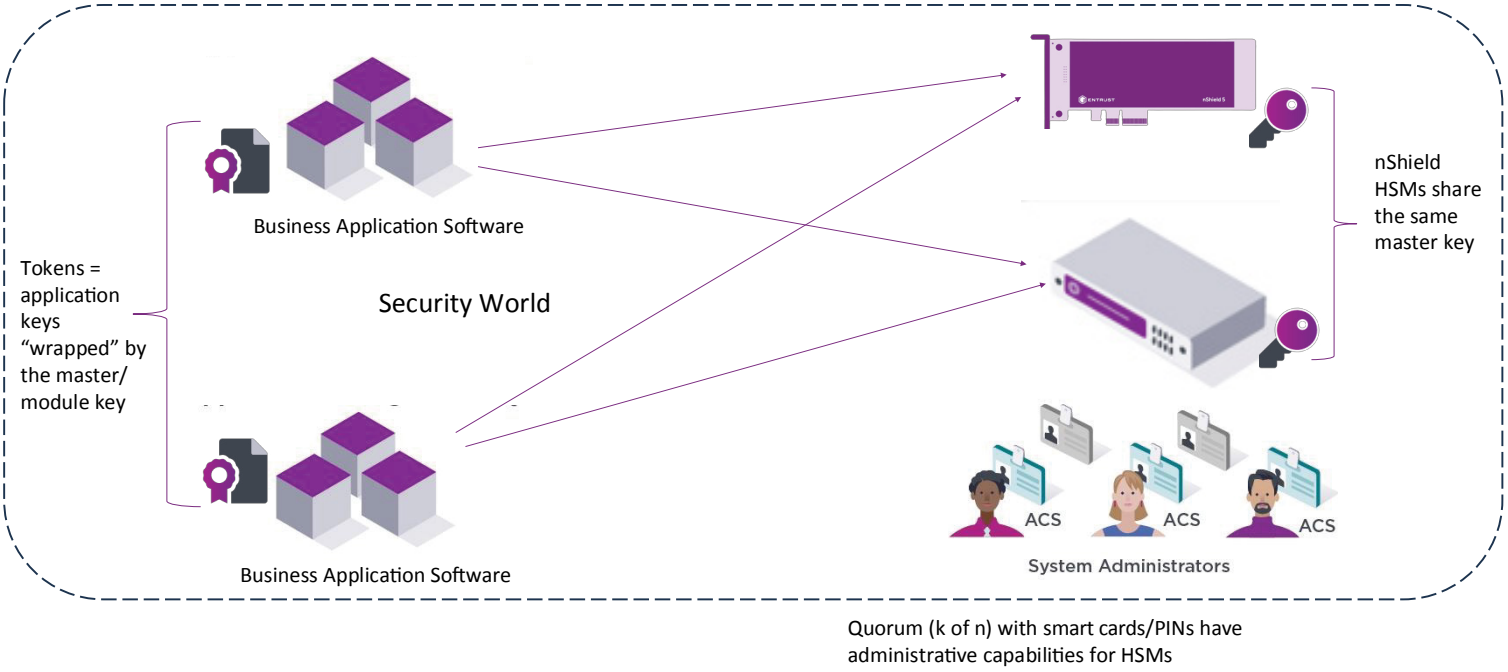


Figure 2: Illustration of Security World Architecture

Multi-Tenant Firmware

To meet the stringent isolation and security requirements of NIST FIPS 140-3 while delivering a versatile multi-tenant nShield HSM, the nShield architecture has been extensively redesigned. Figure 3 below illustrates the multi-tenant firmware architecture, which isolates nCore instances into cryptographically independent Versatile Crypto Modules (VCMs) within the HSM. This makes it possible to run multiple independent cryptographic modules, on a single physical nShield HSM.

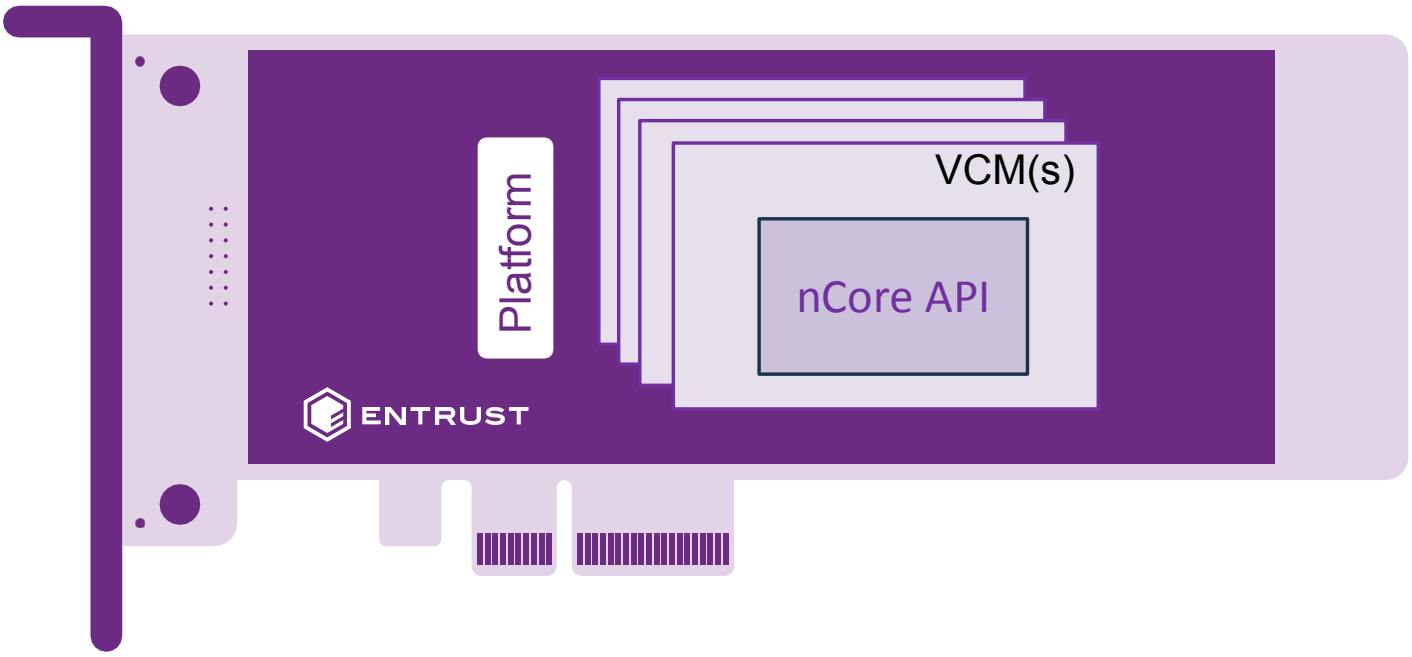


Figure 3: Illustration of multi-tenant firmware on nShield 5s providing containerization of multiple VCM instances

Security Architecture and Isolation Model

nShield Multi-Tenancy is designed to deliver **strong isolation of cryptographic environments on shared HSM infrastructure**, enabling multiple tenants to operate independently while maintaining the security assurances of dedicated HSM deployments.

Scope and Assumptions

This white paper describes the architecture and design principles of nShield Multi-Tenancy.

The following assumptions apply:

- The HSM hardware and firmware are trusted and have not been compromised
- Security controls are correctly configured and maintained throughout the system lifecycle
- The service provider is responsible for infrastructure operation but does not have access to tenant cryptographic material
- External systems (e.g. client hosts, networks) are outside the scope of this document and must be secured independently
- All Security World principles apply to individual VCMs, including client authorization/authentication, individual key Access Control Lists and any additional logical protection tokens, such as Operator Card Sets or Softcards.

These assumptions are important to correctly interpret the security properties described in this paper.

Security Objectives

The architecture is designed to:

- Enforce strong cryptographic isolation between tenants
- Prevent cross-tenant access to tenant keys and operations
- Avoid service provider access to tenant cryptographic material and operations
- Enable independent control and governance of cryptographic environments
- Support mixed compliance and operational requirements on shared infrastructure

Each tenant operates within a dedicated cryptographic environment, with exclusive ownership of keys, policies, and administrative control.

Isolation Model

Isolation in nShield Multi-Tenancy is enforced through the Versatile Crypto Module (VCM) – a containerized instance of HSM functionality operating within the physical device.

Each VCM provides:

- A **dedicated cryptographic execution environment**
- Its own **Security World and protected key storage**
- An independent **instance of HSM firmware and services**

Tenants operate exclusively within their assigned VCM, and the architecture is designed to prevent one tenant from accessing or interacting with another tenant's resources.

This approach is intended to provide strong separation of security domains, rather than logical partitioning within a single shared environment.

Separation of Responsibilities

The architecture enforces a clear separation between infrastructure management and cryptographic ownership:

- **Service provider responsibilities** include hardware operation, lifecycle management, and provisioning of VCMs
- **Tenant responsibilities** include managing Security Worlds, cryptographic policies, and operational use

Once the service provider provisions a "vacant" VCM, and the tenant has loaded their Security World, the service provider has **no access to tenant keys, policies, or cryptographic operations**, eliminating shared trust dependencies.

Protection of Data and Communications

All communication between client systems and the HSM is protected using **authenticated and end-to-end encrypted channels**, terminated within the HSM's security boundary.

Each tenant independently manages its access credentials and sessions, ensuring that:

- Connections are **cryptographically verified and protected**
- Access to services is **restricted to authorized tenant environments**

Device-level attestation mechanisms further ensure that communications originate from a trusted HSM platform.

Resource Sharing and Isolation Boundaries

While different tenants share the same physical HSM hardware, responsibilities are divided as follows:

- **Shared components**: physical compute resources (e.g. CPU, memory, hardware boundary)
- **Isolated components**: key material, Security World data, firmware execution context, and administrative control

This separation is designed to achieve hardware efficiency while maintaining strong cryptographic isolation.

Lifecycle Security

The lifecycle of each tenant environment is managed to preserve security throughout:

- VCMs are provisioned with tenant-specific credentials and configuration
- Cryptographic material is initialized and managed exclusively by the tenant
- When a VCM is deleted, associated data and internal protection keys are securely removed from the system in a manner designed to prevent recovery of tenant cryptographic material

Threat Considerations

The architecture is designed to address the following classes of risk:

- Cross-tenant access to cryptographic material or operations
- Privilege escalation within shared infrastructure
- Misconfiguration leading to unintended access
- Unauthorized access by infrastructure operators

These risks are mitigated through cryptographic isolation, separation of responsibilities, and restricted administrative access. Residual risk depends on correct configuration and operational controls.

Trust Model

nShield Multi-Tenancy is designed to minimize shared trust assumptions by enforcing separation between tenants and between tenants and the service provider.

In this model: Tenants are isolated from other tenants through independent cryptographic environments. The architecture protects tenant cryptographic material from access by the Service Provider. These controls reduce reliance on operational trust between parties.

However, the model assumes:

- Correct system configuration and lifecycle management
- Integrity of the HSM hardware and firmware
- Enforcement of defined administrative boundaries

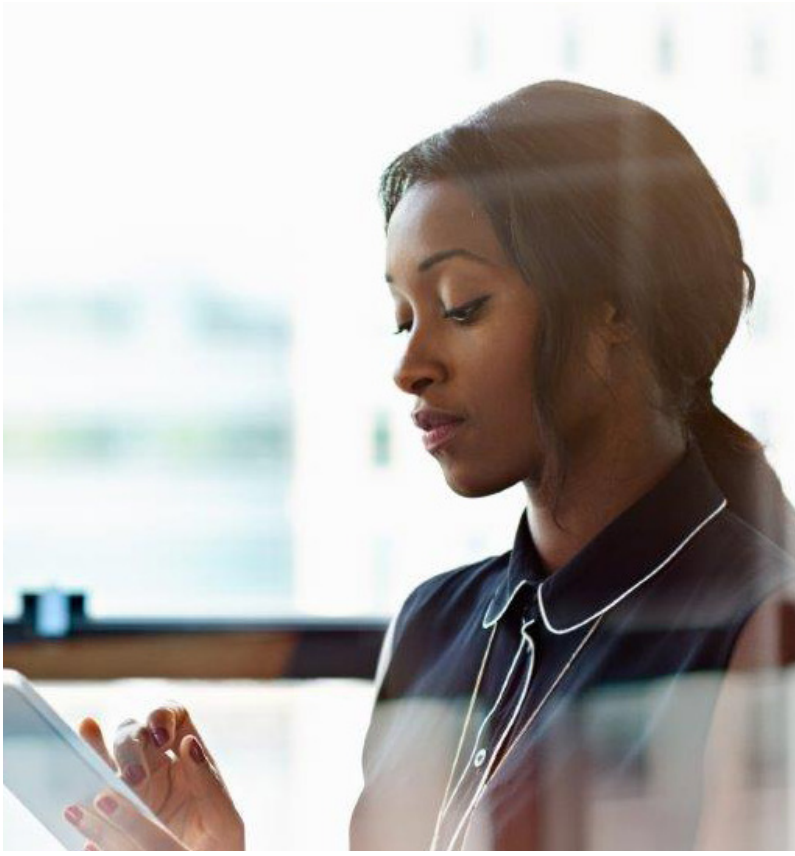
Security boundaries are therefore enforced both by architectural design and by correct operational practice.

Deployment Considerations

In the initial release (June 2026):

- VCM configurations are provisioned and managed by the service provider.
- A single firmware version is supported across all VCMs, with future releases expected to introduce greater flexibility.
- Today, Versatile Crypto Modules (VCMs) share core resources equally. Planned enhancements in future nShield HSM multi-tenancy firmware aim to introduce VCM prioritization, enabling more flexible allocation aligned to workload requirements.

These constraints do not affect the fundamental isolation model but should be considered in deployment planning.



Deployment Use Cases Leveraging Multi-Tenancy

nShield HSM customers range from organizations operating complex, globally distributed multi-Security World environments to those requiring only one or two Security Worlds within a single geographic region, with many variations in between. Before the introduction of multi-tenant firmware, each nShield HSM supported only a single Security World. As a result, customers were forced to choose between consolidating multiple client applications into one Security World – reducing the level of isolation – or deploying additional HSMs to maintain separation across Security Worlds.

With these capabilities now available, customers can tailor their deployment models to operational needs. For example, global organizations may choose to deploy dedicated HSMs to high-volume transaction services while consolidating multiple Security Worlds onto fewer HSMs in lower-volume transaction applications.

Use Case	Security Objective	Isolation Mechanism	Primary Benefit
Multi-Application Consolidation	Separate application trust domains	Dedicated VCM per application	Reduced HSM footprint
Data Center Consolidation	Maintain isolation for low-volume services without dedicated HSM units	Independent Security Worlds	Lower operational costs

Use Case 1: Single multi-tenant HSM serving multiple applications

One of the most common use cases for multi-tenant HSMs is to achieve strong cryptographic separation between applications while consolidating onto fewer physical hardware platforms. This approach is not appropriate in every scenario, as feasibility depends on the transaction demands of the applications being consolidated. Applications with lower transaction volumes – such as document signing or code signing – are often well-suited to this model. With nShield 5s, this can be implemented through multiple virtualized applications running on a single physical server, with cryptographically isolated Versatile Crypto Modules (VCMs) deployed within a single nShield 5s. Technically, this configuration can also support applications on separate physical hosts, as long as they are on the same LAN subnet or across multiple nShield 5s devices (see Figure 4) in the same server.

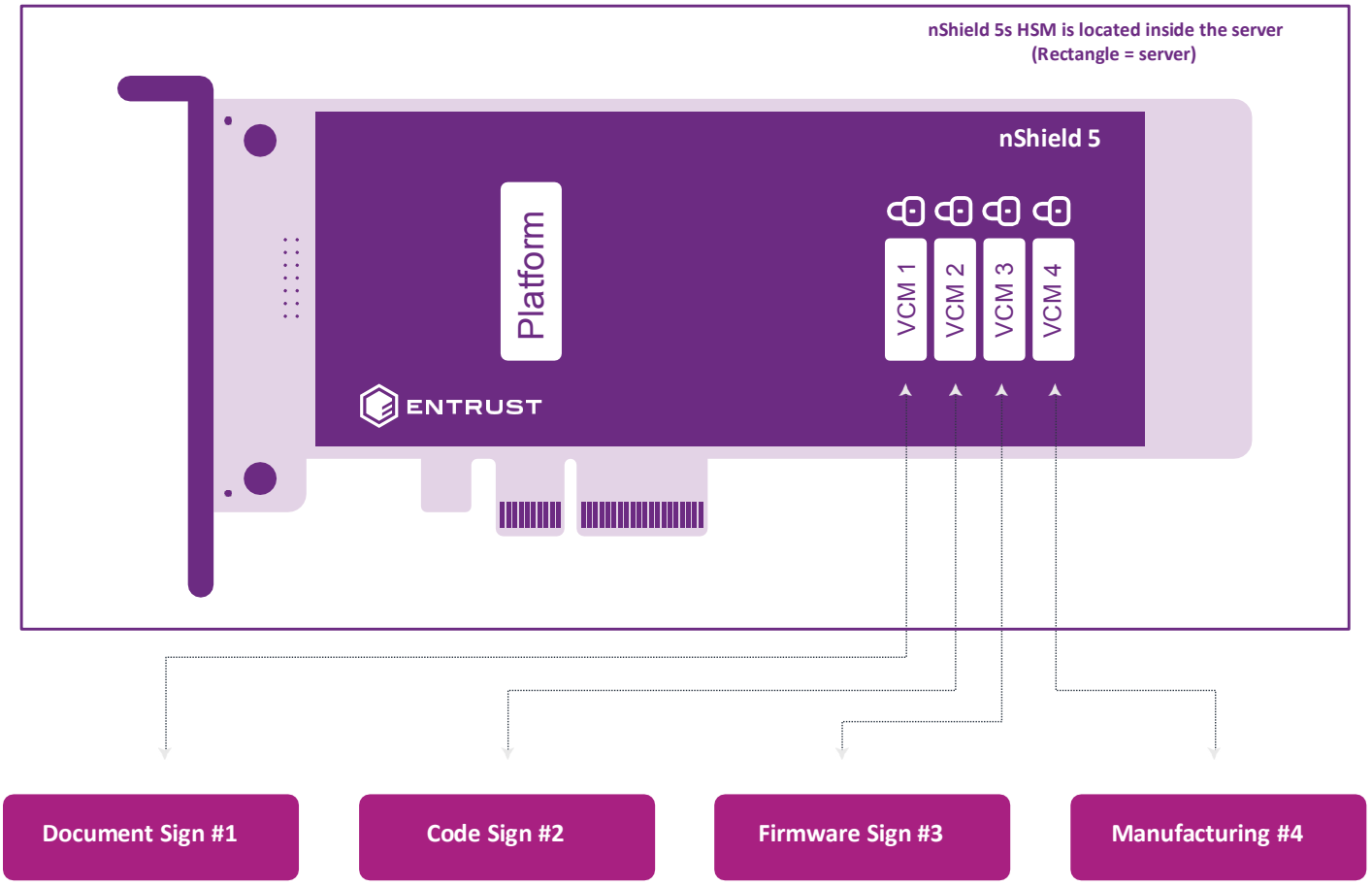


Figure 4: Illustration of a single nShield HSM supporting multiple virtualized applications

Use Case 2: Consolidating HSMs in data center

In some scenarios, applications with high cryptographic demand in the data center require significantly less performance in backup locations. In these cases, the primary data center may retain a dedicated HSM for each application, while backup data centers consolidate multiple applications (as VCM) and their associated cryptographic modules onto a single hardware platform to reduce cost, optimize data center space, and simplify operations. Again, it is possible to have the applications running in their own hosts, provided they are on the same LAN segment as the nShield 5s HSM's host.

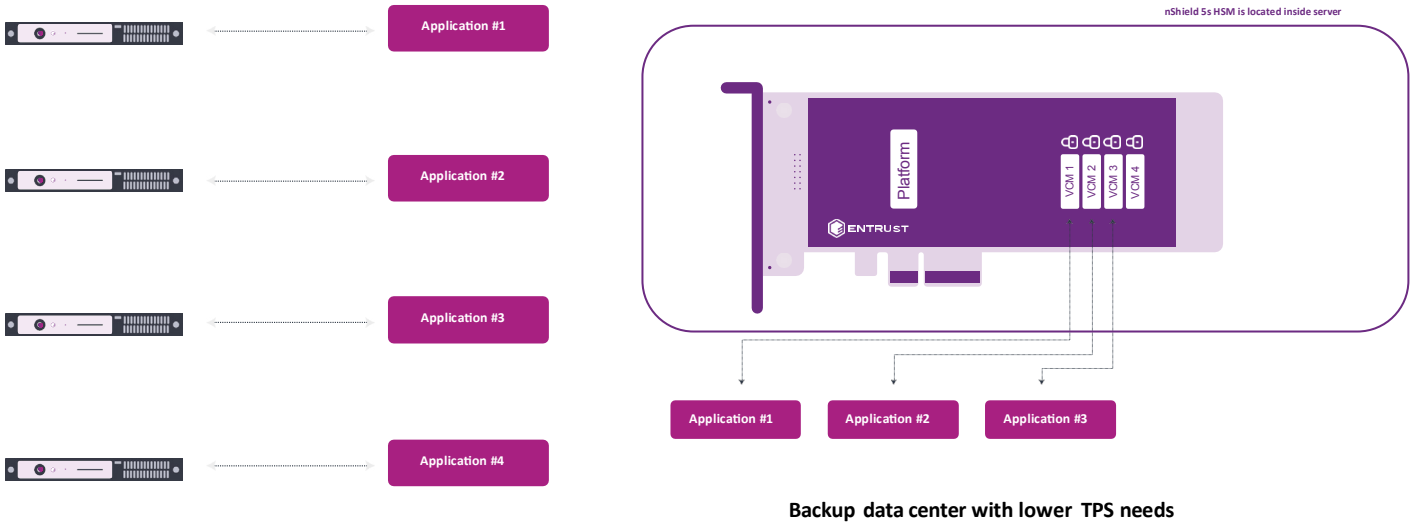


Figure 5: Consolidating HSMs in backup data center deployments

Multi-Tenancy on the nShield 5s

Figure 6 below illustrates the nShield 5s architecture in a multi-tenant configuration.

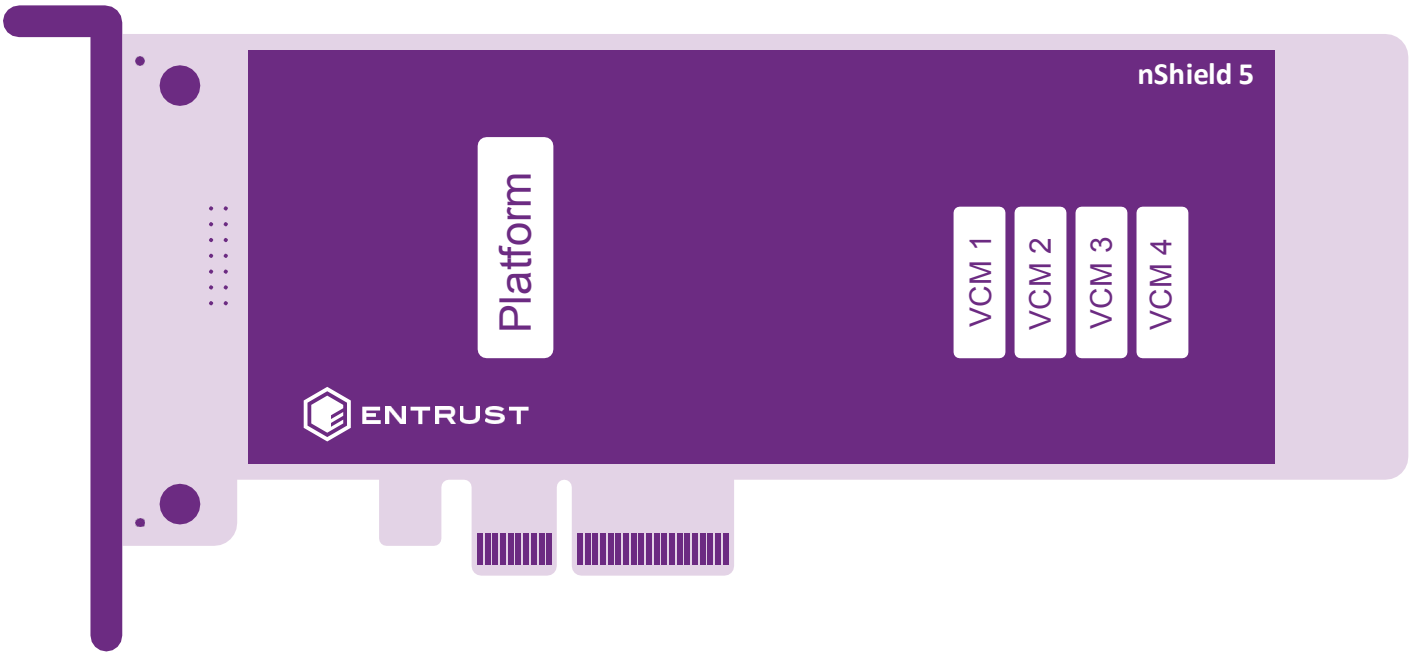


Figure 6: Illustration of the platform and client services in the nShield multi-tenant architecture

The Versatile Crypto Module (VCM)

The nShield 5s firmware separates the functions that manage Security World data from those that manage the physical HSM platform. The core difference between the nShield 5s single-tenant firmware and multi-tenant firmware is that, in multi-tenant firmware, multiple ncoreapi service containers can be provisioned by the service provider. Each independent instance of the ncoreapi service and its associated data is packaged into a container called a Versatile Crypto Module (VCM). Multiple VCMs can run in parallel on a single HSM, sharing underlying hardware resources while remaining independently addressable through the HSM APIs.

- Each VCM has its own protected key storage and its own firmware instance.
- A VCM can host a single Security World, and multiple Security Worlds can coexist on the same physical HSM running in separate VCMs.
- No tenant can access another tenant's resources, so each VCM operates as a cryptographically isolated environment.

Each tenant can operate its Security World in the mode required for its environment. For example, one Security World can run in unrestricted mode while another runs in strict FIPS or Common Criteria mode. Each Security World requires its own Administrative Card Set (ACS). Standard logical tokens are also supported, including Softcards and Operator Card Sets where key-generation policy requires them. For Security World administrators and client hosts, each VCM behaves the same way as a dedicated single-HSM deployment.

Note: In the initial release, all VCMs must run the same firmware version (for example, v14.x). Future releases are expected to support different firmware versions per VCM, giving customers greater flexibility for development, testing, and migration scenarios.

Tenant isolation

Tenant isolation is enforced through a layered combination of containerization, operating system controls, and hardware-enforced boundaries that restrict execution, memory access, and communication between tenants.

- Execution environments are isolated to prevent interaction between tenants
- System interfaces and privileges are restricted to enforce least-privilege operation
- Communication between tenants is prevented unless explicitly authorized

Additional VCM services

Each VCM includes its own supporting management services in addition to the ncoreapi service. These local instances provide monitoring and credential administration within the VCM, while remaining isolated from both system-level services and other VCMs.

- The monitor service provides access to log messages generated by the VCM's ncoreapi service, which are stored locally within that VCM rather than in the global system log.
- The sshadmin service manages the VCM's SSH client credentials, allowing access to ncoreapi and monitor to be administered independently for each VCM.

This design keeps operational logs and access credentials bounded to each VCM, enabling independent administration without exposing data or control across tenant boundaries.

A new service called orchestrator creates and manages VCMs. Its corresponding host-side tool is vcmadmin, as shown in the diagram on the following page.

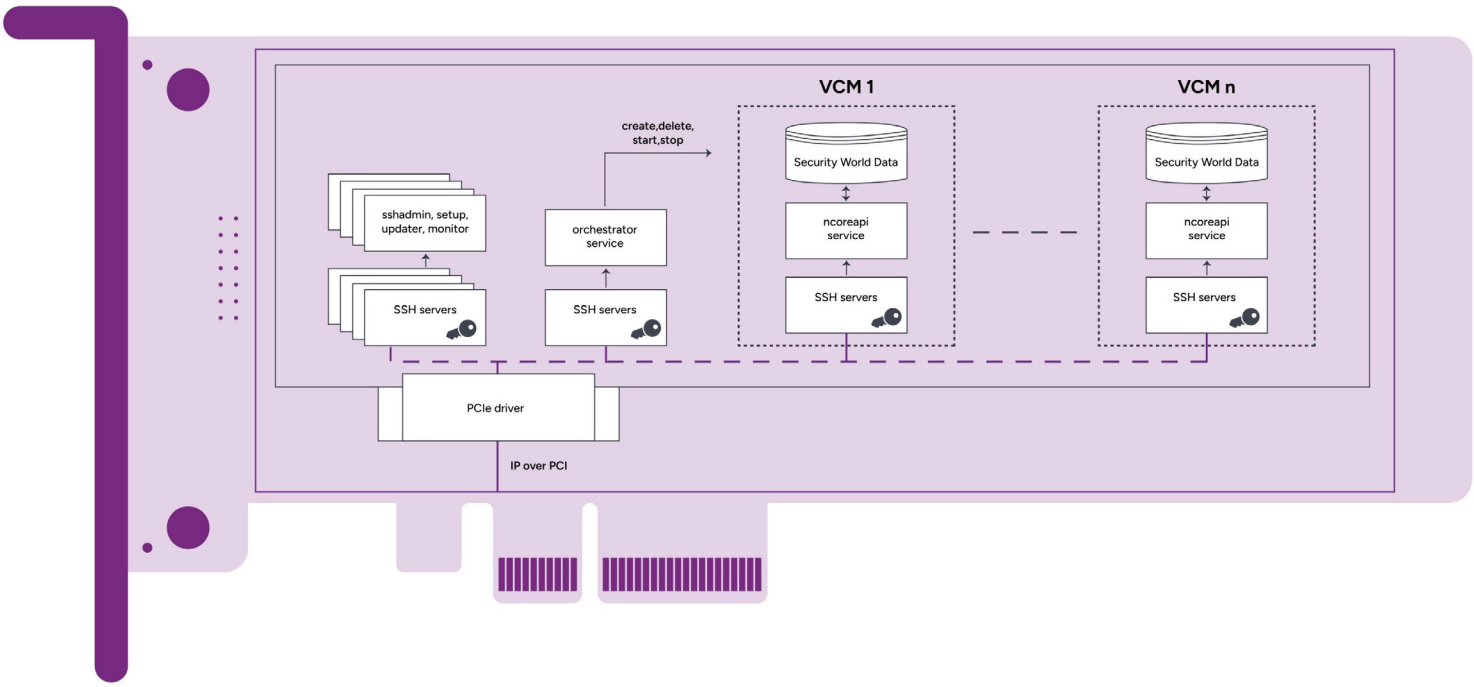


Figure 7: Additional VCM services for multi-tenancy

Service provider and tenants

In a multi-tenant HSM deployment, two roles must remain clearly separated: the **Service Provider**, which owns and operates the physical HSM infrastructure, and the **Tenant**, which uses an assigned VCM for cryptographic operations. This separation ensures that infrastructure control and cryptographic ownership remain distinct.

Responsibilities are divided so that each party manages only the functions within its own boundary:

- **Service Provider responsibilities**: hardware installation and configuration, firmware upgrades and maintenance, health monitoring, and creating or removing VCMs on behalf of tenants.
- **Tenant responsibilities**: establishing VCM SSH client credentials, loading and managing Security Worlds, using the VCM to deliver cryptographic services to applications, and collecting audit logs for that VCM.

Within both service provider and tenant organizations, these activities can be assigned to separate user roles. In practice, tasks such as health monitoring and audit log collection are often automated, and the credentials used for those tasks can be restricted so they do not grant broader administrative privileges.

Once a VCM has been provisioned, the service provider cannot access its internal environment. It cannot change tenant-defined credentials, access the ncoreapi service, or retrieve logs generated within that VCM.

Together, tenant-controlled credentials, VCM isolation, and network separation help ensure that service provider and tenant domains remain distinct throughout operation.

Attestation of SSH keys

The nShield 5s HSM is provided with its own signing key pair, unique per device, which is certified ("warranted") during manufacture. All SSH keys generated by the HSM have a certificate signed by this key pair, which forms a chain of trust back to Entrust. These certificates are checked by the tools when connecting to the HSM, assuring any user of HSM services the connection is not being spoofed by an attacker.

VCM lifecycle (dynamic capability future)

In the initial nShield 5s multi-tenancy release, the VCM lifecycle is service provider-managed and largely static. Future releases are expected to introduce a more dynamic model, allowing pre-provisioned standby VCMs to be started, stopped, and reassigned more flexibly as demand changes.

The VCM lifecycle consists of four main stages:

- **Creation**: The service provider creates the VCM for a new or existing tenant using a tenant-supplied initial SSH public key for sshadmin, assigns operational properties such as IP address, enabled features, and performance controls, and the HSM generates a UUID to identify the VCM in later operations.
- **Initialization**: After the VCM starts, the tenant uses sshadmin to set client SSH credentials for monitor and ncoreapi. The tenant then uses Security World tools to initialize ncoreapi and load Security World data, making the VCM ready for application use.
- **Start/stop**: The service provider can start or stop a VCM through the orchestrator service. When stopped, the VCM retains only a small amount of non-volatile storage and does not consume CPU, memory, or other active HSM resources, enabling large numbers of inactive VCMs to be held in reserve.
- **Deletion**: When a tenant no longer requires service, the service provider can delete the VCM to free its non-volatile storage. The HSM also securely removes the internal keys protecting the VCM's SSH credentials and Security World data, fully removing the tenant's presence from the system.

In future releases, service providers are expected to be able to pre-provision VCMs for specific applications and shift capacity dynamically across HSMs as workloads change. This would support burst capacity, standby deployments, and highly resilient operating models, with start and stop actions that can be automated in orchestration frameworks such as Kubernetes.

Firmware upgrade behavior (future)

In earlier HSM generations, upgrading or downgrading firmware erased Security World data. In future multi-tenant deployments, a VCM's Security World data can be marked persistent, so it survives a firmware upgrade, avoiding the need to reinstall a VCM after a firmware update. This approach reduces upgrade disruption while preserving tenant control over whether persistence is appropriate for their compliance model.

Networks and connections

Each tenant is expected to run client software in a compute environment separate from the service provider's. To support this, every VCM is assigned its own endpoint connection with a separate IPv4 or IPv6 address, which can be routed from the host to an external network. Each client has its own end-to-end encrypted tunnel with the HSM, which guarantees a strong level of separation between the VCM at the network level as well. In the initial nShield 5s HSM deployment model, networking is restricted to the same LAN subnet or virtualized applications within a single server. Future versions of multi-tenant firmware will be released to enable nShield 5c HSM models to operate at scale in much broader networked configurations.

Why nShield Multi-Tenancy?

Traditional Partitioning	nShield Multi-Tenancy	Multi-Tenancy Benefits
Shared trust boundary	Independent trust domains	Eliminates shared security dependencies between tenants and strengthens isolation.
Shared admin model	Tenant-controlled Security Worlds	Provides tenant autonomy, ownership of cryptographic assets, and separation of duties.
Policy-based separation	Architectural separation	Delivers stronger isolation through dedicated cryptographic environments rather than logical controls alone.
Greater operator trust dependency	Reduced operator trust dependency	Minimizes insider risk and reduces reliance on infrastructure operators for security.
Shared firmware environment	Independent firmware instances	Limits the impact of software defects, misconfigurations, and privilege escalation events.
Limited or no SLA guarantees	Each tenant has its own performance rates to guarantee SLA and avoid service disruptions.	Tenancies can be activated in 3 modes: as an nShield 5 Base: max speed is equivalent to nShield 5s Base, Mid or Auto (max speed can be up to max HSM capacity)

Some alternative HSM vendors implement multiple tenants using application partitions, which provide separation of cryptographic objects and access through roles (Partition Security Officer, Crypto Officer, and Crypto Users) and policy controls. Each partition acts as a logically distinct container for keys and operations. Access is constrained by authentication and policy enforcement. This is similar to nShield's Operator Card Sets, where a key or group of keys and their integral Access Control Lists are put under another cryptographic layer of protection. This is implemented using a logical token that is broken into a shared secret requiring a quorum to load and use the key(s). In both models, keys are securely separated and governed by well-defined roles and access controls, but they remain part of a single administrative and operational domain. The overarching HSM administrator retains authority over system-level configuration, updates, and system resets.

nShield multi-tenancy isolates administrative control from cryptographic operations. The service provider role provisions and operates the physical HSM platform, but once a VCM is allocated and initialized, the tenant alone controls its Security World, keys, and policies. The architecture is explicitly designed so that the infrastructure operator does not have access to tenant key material, policies, or cryptographic operations. This reduces reliance on operational trust and introduces a clearer separation of security responsibilities between infrastructure operators and tenants.

With alternative vendors partitions operate within a shared firmware environment, where isolation depends on correct enforcement of roles, policies, and access controls across partitions. By comparison, the nShield approach isolates tenants at multiple layers:

- Independent firmware and service instances per VCM
- Segregated execution environments
- Controlled communication boundaries between tenants

This architectural separation reduces the potential impact of system-level misconfiguration, privilege escalation, or software defects. The key difference lies in scope:

- In the partition model, policies are applied **within a shared trust boundary**.
- In the VCM model, policies are applied **within independent trust domains**, eliminating shared policy dependencies between tenants.

Furthermore, with some alternative vendors, certain partition lifecycle operations, such as reinitialization or specific policy changes, may require **destructive actions**, including deleting all cryptographic objects within the partition. As a result, dedicated backup devices are required for each partition to ensure the environment and its cryptographic objects can be restored to a previous state.

Entrust Multi-Tenancy manages lifecycle at the VCM level. Each tenant environment is created, initialized, operated, and even deleted independently. When a VCM is removed, associated cryptographic material and internal protection keys are securely deleted to prevent recovery. Of course, Entrust recommends that all mission-critical HSM estates be redundant at the Security World level to ensure any kind of failure at the hardware level or within a data center environment aren't catastrophic to all Security World members. And a Security World at the HSM level can always be recovered by the action of the Administrative Card Set holders to simply re-enroll the Security World into a vacant VCM or a physical, dedicated HSM.

Entrust's multi-tenant architecture introduces several security advantages in environments where tenant independence and trust minimization are critical:

- **Stronger isolation boundary**
  Isolation is implemented as independent cryptographic environments rather than logical separation within a shared system.
- **Reduced operator trust dependency**
  Infrastructure operators cannot access tenant keys or cryptographic operations once environments are provisioned.
- **Independent trust domains**
  Each tenant controls its own Security World, policies, and administrative processes.
- **Reduced cross-tenant risk**
  Architectural separation minimizes the potential impact of software defects, misconfiguration, or privilege escalation at the system level.

Entrust provides a more powerful and flexible model based on distributed trust. The nShield architecture removes a single persistent master key and instead uses quorum-based smart cards (Security World), significantly reducing the risk of a single-point compromise.

nShield Multi-Tenancy also addresses several real-world operational pain points that can create friction in enterprise environments. For example, because key material and trust are not bound to a single device, organizations can recover or rebuild entire environments – including individual tenants – independently of specific hardware. This significantly simplifies disaster recovery, hardware replacement, and platform migration, all of which are traditionally high-risk and operationally disruptive activities. Tasks such as migrating workloads between data centers, scaling into cloud environments, or replacing aging HSMs can be performed without tightly coupling operations to a specific appliance or requiring complex rekeying exercises. This reduces downtime, lowers operational risk, and avoids the coordination overhead that typically burdens crypto officers during major lifecycle events.

While nShield Multi-Tenancy requires stronger upfront governance, it can materially reduce friction over time by reducing the dependencies associated with rigid hardware-bound processes. For organizations operating multi-tenant or service-provider models – particularly where strong isolation, regulatory separation, or reduced operational trust is required – this architectural distinction represents a meaningful advancement in HSM multi-tenancy security. When coupled with nShield's ability to add further layers of logical separation of keys using OCS and Softcard protection for keys, significant flexibility in implementing key and security domain isolation can be achieved.

Planning Your Multi-Tenant Deployment

To plan a multi-tenant deployment, you first need to assess your current HSM estate. Start by evaluating client applications and the load they generate in each location where HSMs are installed. You should also account for planned changes, such as data center migrations, post-quantum cryptography initiatives, and new applications coming online. Understanding where compliance requirements differ across applications is equally important.

Multi-Tenancy is a journey, not necessarily the destination for every HSM requirement. Entrust Professional Services can help you assess your environment, gather the necessary telemetry, and plan an implementation that fits your operational and compliance needs.

Conclusion

nShield Multi-Tenancy is designed to provide strong cryptographic isolation within shared HSM infrastructure. By separating cryptographic ownership from infrastructure control and enforcing boundaries between tenants, the architecture enables more efficient use of hardware while maintaining a high level of security assurance and proper resource allocation to avoid service disruptions. As with any multi-tenant system, achieving these properties depends on correct configuration, operation, and lifecycle management.

Glossary of Terms

For clarity and for those general-interest readers unfamiliar with the subject, here is a high-level definition of some of the terms used within this paper:

Security World

A Security World defines the fundamental cryptographic trust boundary within an nShield HSM environment.

It determines how cryptographic keys are created, protected, and governed, including the policies, administrative controls, and authorization mechanisms that apply to those keys. Security Worlds are protected using quorum-based smart card mechanisms, ensuring strong separation of duties and preventing unilateral administrative control.

In a multi-tenant environment, each tenant operates within its own independent Security World, ensuring that cryptographic assets and policies remain fully isolated.

Read more on Entrust **Security World** architecture.

Tenant

A **tenant** is an independent entity – such as an application, business unit, or external customer – that uses HSM services to perform cryptographic operations.

Each tenant:

- Controls its own Security World
- Manages its own keys and policies
- Maintains independent administrative control

Tenants operate without visibility into, or dependence on, other tenants sharing the same physical HSM infrastructure.

Versatile Crypto Module (VCM)

A **Versatile Crypto Module (VCM)** is an isolated, containerized HSM instance running within a physical nShield HSM.

Each VCM provides:

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

A VCM behaves as a logically separate HSM, even though it shares underlying hardware resources with other VCMs. This allows multiple tenants to coexist securely on a single device, without sharing cryptographic state or administrative control.

Service Provider

A service provider is the entity responsible for owning and operating the physical HSM infrastructure.

The service provider:

- Manages hardware installation, configuration, and maintenance
- Creates and allocates “vacant” VCMs to tenants
- Monitors system health and overall platform operation

Importantly, the service provider does not have access to tenant cryptographic assets, keys, or Security World data once a VCM has been provisioned with a tenant’s Security World.

Platform Services

Platform Services refer to the set of operational functions required to manage the underlying HSM infrastructure.

These services include:

- Hardware lifecycle management (installation, upgrades, maintenance)
- System monitoring and health management
- Provisioning and lifecycle management of VCMs

Platform Services are distinct from tenant-controlled cryptographic operations and do not provide access to tenant environments.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

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

ENTRUST
SECURING A WORLD IN MOTION