

DATASHEET

nShield as a Service

Easy, efficient access to high-assurance cryptography as a service

HIGHLIGHTS

- Hosted, managed HSM service in a PCI-DSS certified cloud deployment¹
- Post-quantum support is provided by the nShield HSMs used in nShield as a Service to support NIST quantum-resistant algorithms
- Future-proof your cryptographic services with included firmware upgrades that enable future algorithm support and hardware acceleration
- Maintain full control over key material regardless of where application workloads are running
- Extend cloud-based cryptography and key management across multiple clouds
- Support secure code execution for cloud-based workloads
- Meet geo-fencing requirements for cloud data security and data sovereignty mandates via regional data centers
- Use Cloud Disaster Recovery (CDR) option to increase redundancy and reliability of on-premises deployments

In today's fast-moving enterprise IT environment, "cloud-first" is a common strategic aim of many organizations. Gone are the days when companies automatically host their critical IT infrastructure on premises. With the shift to the cloud, organizations benefit from the scale, flexibility and resilience of a cloud service provider while enjoying a reduced maintenance burden and a more predictable monthly operational expense.

This business shift results in tension when cloud applications rely on hardware security modules (HSMs), physical appliances that protect the cryptographic keys that act as the root of trust for an organization's encrypted data. Traditionally housed in redundant data centers and managed by an on-site security team, HSMs help customers meet regulatory or certification requirements and are an important part of an organization's critical infrastructure.

Given the increasing demands on enterprise security teams, finding skilled security professionals to administer HSMs is an ongoing challenge. nShield as a Service provides the same features and functionality as on-premises HSMs combined with the benefits of a cloud service deployment. This allows customers to fulfill their cloud-first objectives and leave the management and maintenance of these appliances to the experts at Entrust.



¹ nShield as a Service is PCI-DSS certified in the United States Region

Cryptography as a service

nShield as a Service is a subscription-based solution for generating, accessing, and protecting cryptographic key material, separately from sensitive data. The solution uses FIPS 140-2/140-3 and eIDAS

(EN 419 221-5) certified nShield network attached HSMs in a PCI-DSS certified cloud-hosted model. This gives organizations the option to either supplement or replace HSMs in their data centers while retaining the same benefits as owning the appliances. nShield as a Service allows enterprises to budget for security more predictably, manage capacity based on demand, reduce their data center footprints, and decrease the time spent on routine maintenance and monitoring tasks.

Subscribed customers interact with the cloud-based HSM Service in the same way that they would with appliances in their own data centers, but have no need to receive, install, and maintain physical hardware. This often results in a shorter time between initial procurement and use of the HSM Service and, therefore, faster deployment of secured applications.

Aligns with your security strategy and demands

nShield as a Service is well-suited to align with any security strategy, whether an organization is adopting a cloud-first approach for its cryptographic functions, selectively migrating specific services to the cloud, or enhancing HSM capacity to handle occasional workload spikes.

Because nShield as a Service benefits from the same unique Security World architecture as on-premises nShield deployments, customers can use a hybrid approach, mixing both nShield as a Service and on-premises HSMs. nShield Security World is a scalable key management framework that spans the customer's nShield estate and provides a unified administrator and user experience and guaranteed interoperability across all devices, whether subscription-based or owned on-prem.²

This allows customers to easily and efficiently scale their HSM operations with their specific environment, operational approaches, and security needs. Additionally, the unique CodeSafe secure execution capability gives customers on-demand access to expanded secure computing capacity. Only nShield as a Service allows customers to seamlessly migrate their secure code execution from an on-prem HSM to the cloud.

The nShield as a Service difference

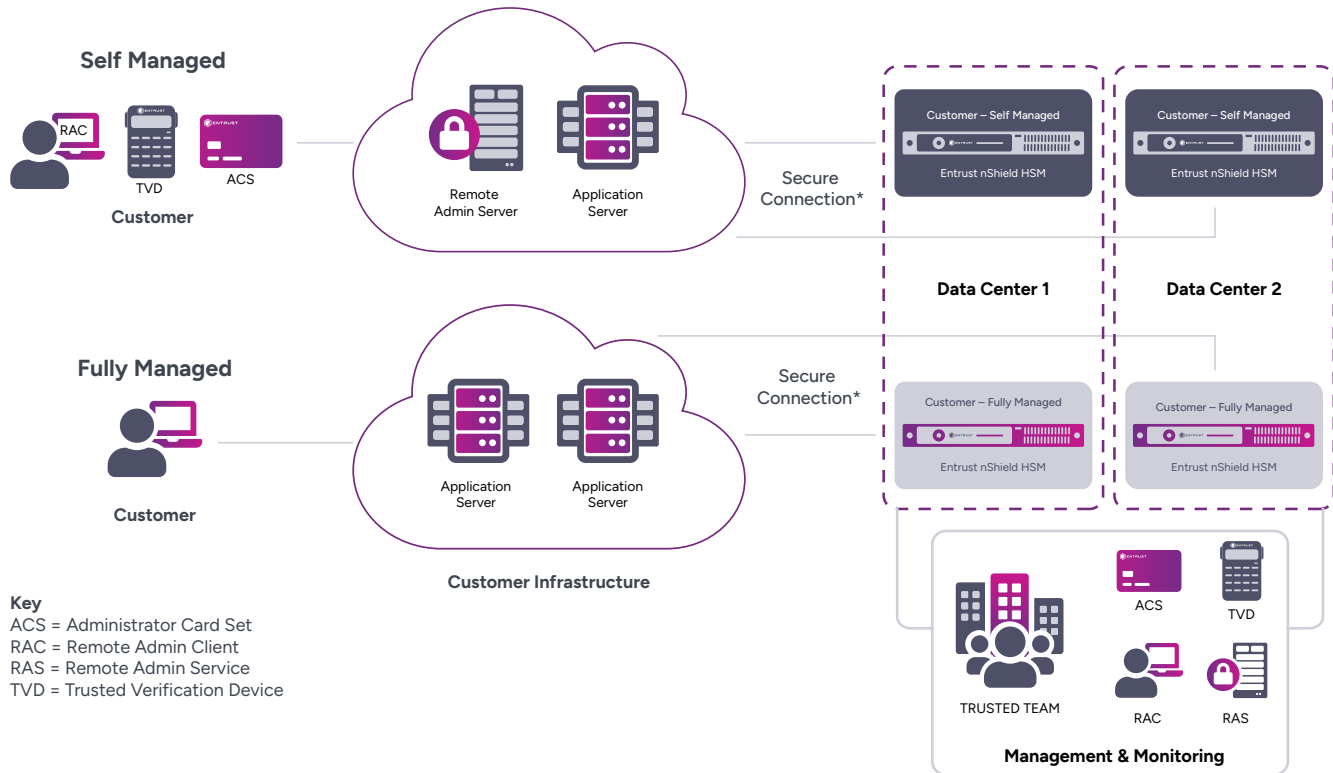
nShield as a Service offers several key advantages over competing options:

- Ensures customers own their Security World resources and keys and may use these across their nShield environment, whether as-a-service or on-premises
- Provides customers on-demand control to migrate and expand their secure code execution from an on-prem HSM to the cloud
- Delivers FIPS 140-2/140-3 Level 3 and eIDAS (EN 419 221-5 protection profile) certified security of keys, which is not available with some cloud key protection solutions
- Enables customers to continue using the same business applications with their cloud-based nShield service and have the option to access enhanced HSM capacity to handle occasional workload spikes
- Deploy with multiple cloud service providers, in contrast to HSM services offered by individual providers that can lock customers into their own cloud environments. Supports hybrid cloud deployments and offers easy key migration should data repatriation from a cloud service provider to on-prem be required.
- Customers have full control of their cryptographic keys – full separation of duties ensures no individual can single-handedly change key use policies

² See for further info.

nShield as a Service deployment options and features

nShield as a Service is available in a range of different feature/performance levels to enable customers to match capabilities to their operational, disaster recovery, and data sovereignty needs while choosing the optimum performance and price point. Self-managed or fully-managed deployment options are also available for greater flexibility (see diagram).



NSHIELD AS A SERVICE PERFORMANCE TIERS AND MANAGEMENT OPTIONS

Performance Tier	Basic	Standard	Premium	Enterprise
Indicative performance (2K RSA signatures per second)	400 tps	800 tps	6,000 tps	16,000 tps
Number of deployments	1	2	2	2
High Availability – multi-geographical locations		•	•	•
Committed SLA	99%	99.9%	99.9%	99.9%
Number of concurrent application Sessions	3	10	25	50
Available as a fully managed option		•	•	•

A Cloud Disaster Recovery solution is also available, enabling organizations with in-house HSM estates to easily increase the redundancy and resiliency of their deployments, without having to add in-house equipment and personnel resources. Offered as a cost-effective, subscription-based solution, the Cloud Disaster Recovery solution has a 99% SLA, multi-geographical locations, and ten concurrent application sessions.

Management Options	Self Managed	Fully Managed
Customer has access to nShield network attached hardware hosted in secure data center	✓	✓
The nShield Remote Administration kit lets you securely connect to and interact with your cloud-based nShield HSM(s)	✓	✓
24/7 Premium Maintenance & Support	✓	✓
Full management of Security World Installation • nShield Security World creation • Security Officer role fulfilled by Entrust personnel • Firmware updates • Configuration updates as requested		✓
• Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) – Level 1 & CSA Trusted Cloud Provider • PCI-DSS (US)	✓	✓

Technical Specifications

Connectivity

- IPsec tunnel w/ pre-shared keys between customer Cloud IP spaces and managed nShield HSM environment
- Transparent to client hosts
- Takes entire path out of control scope

Certified Hardware Solutions

nShield as a Service is built with nShield HSMs that help our customers demonstrate compliance while also giving them the assurance that their HSMs meet stringent industry standards.

nShield Features

nShield as a Service delivers the same features as on-premises nShield HSMs, including CodeSafe, Web Services Option Pack, Container Option Pack, and Database Option Pack.

Security Compliance

- FIPS 140-2/140-3 Level 3
- PCI DSS

Safety and Environmental Standards Compliance

- UL, CE, FCC, RCM, Canada ICES
- RoHS2, WEEE

Data Center Certifications

Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) – Level 1

Wide Support for APIs, Cryptographic Algorithms, and Platforms

APIs

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG and Web Services

Cryptographic Algorithms (Partial List)

- NIST standardized post-quantum algorithms
- Asymmetric public key algorithms: RSA, Diffie-Hellman, ECMQV, DSA, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph), Secp256k1
- Symmetric algorithms: AES, AES-GCM, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, Triple DES
- Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160
- Full Suite B implementation with fully licensed ECC including Brainpool and custom curves

nShield HSMs offer support for the majority of these cryptographic algorithms including PQC as part of the standard feature set. For organizations wishing to use ECC or South Korean algorithms, optional activation licenses are needed.

Operating Systems

Microsoft Windows and Linux operating systems including distributions from Red Hat, SUSE, and major cloud service providers running as virtual machines or in containers.



1 nShield as a Service is PCI-DSS certified in the United States Region