SOLUTION BROCHURE

nShield® General Purpose Hardware Security Modules

ENTRUST

SECURING A WORLD IN MOTION

Contents

Security You Can Trust

Entrust nShield hardware security modules (HSMs) are hardened, tamper-resistant devices that protect your company's most sensitive data. These FIPS-certified modules perform cryptographic functions such as generating, managing, and storing encryption and signing keys, as well as executing sensitive functions within their protected boundaries.

A powerful addition to your security stack, nShield HSMs help you:

- Achieve higher levels of data security and trust
- Meet and exceed important regulatory standards
- Future-proof data security with quantum-secure technology

The nShield Family

To suit your specific environment, the nShield family of general purpose HSMs includes the following models:

Network-attached HSMs

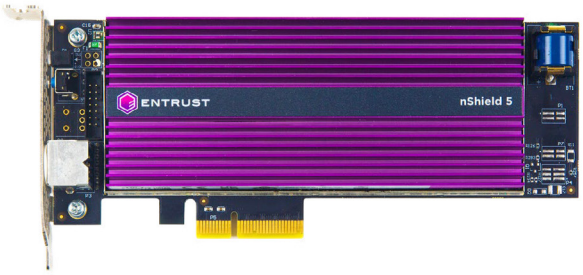
nShield HSMs that deliver cryptographic services to applications distributed across the network. Available in the powerful newer nShield 5c models and established nShield Connect XC models.

Portable USB HSMs

nShield Edge HSMs are desktop devices designed for convenience and economy. They are ideal for developers and support applications such as low-volume root key generation.

PCIe Embedded HSMs

nShield HSMs in a low-profile PCIe card form factor that deliver cryptographic services to applications hosted on a server or appliance. Available in a range of newer, high-specification nShield 5s models and established nShield Solo XC models.



nShield as a Service

A subscription-based model that provides access to dedicated FIPS-certified nShield HSMs. It delivers the same features and functionality as on-premises HSMs – including support for post-quantum algorithms – combined with the benefits of a cloud service deployment. This allows customers to fulfill their cloud-first objectives and leave the maintenance of these appliances to the experts at Entrust.

With nShield as a Service, you own your keys (not the HSM). And because it uses the same unique Security World key management architecture as on-premises nShield HSM deployments, you can easily migrate your cryptographic operations from on-premises to the cloud – or use a hybrid approach, mixing on-premises and cloud-based HSMs for increased redundancy and reliability.

nShield as a Service is available across fully redundant data centers in the EU (Germany), the UK, USA, and Australia. Regional data centers facilitate geo-fencing to meet cloud data security and data sovereignty mandates. A range of service options are offered to meet a variety of customer needs. For price-sensitive customers, a self-managed single HSM instantiation is available in the customer's preferred location. Standard, Premium, and Enterprise customers can specify preferred HSM locations to meet their operational, disaster recovery, and data sovereignty needs while choosing the optimum performance and price point.

Support for a Wide Variety of Uses

Entrust customers use nShield HSMs as the root of trust in a variety of business applications including:

- Public key infrastructures (PKIs)
- TLS/SSL encryption key protection
- Code signing
- Digital signing
- 5G telco applications
- Blockchain

As growth in the Internet of Things (IoT) creates greater demand for device IDs and certificates, nShield HSMs will continue to support critical security measures such as device authentication using digital certificates.

nShield HSMs also support a wide range of cryptographic algorithms, including:

- **New NIST standardized quantum-resistant algorithms** to help you prepare for a post-quantum future
- **Elliptic-curve cryptography algorithms** ideally suited for today's low-power computing environments such as smart meter devices
- **5G compatible algorithms** for telco applications

Features of the nShield HSM Family

Cloud-friendly web service interfaces

The nShield Web Service RESTful interface offers an innovative approach to deployments by removing the need to integrate applications directly with nShield HSMs, and eliminates dependencies on OS and architecture design choices.

Post-quantum secure

The nShield HSM family is designed to help organizations prepare for the quantum future through support of postquantum cryptographic algorithms. Aligned with NIST's Post-Quantum Cryptography Standardization, nShield HSMs enable you to adopt quantum-resistant security with hardware-accelerated performance.

Containerized support on premises or in the cloud

The nShield Container Option Pack enables the seamless development and deployment of containerized applications or processes underpinned by our high assurance HSMs. This option provides a set of pre-packaged scripts that greatly simplify the integration of nShield HSMs into a container application environment while supporting the dynamic, scaling needs of your applications and containerized hosts.

Stronger key management for your cloud data with the Entrust nShield Cloud Integration Option Pack

Supporting Bring Your Own Key (BYOK) deployments, the nShield Cloud Integration Option Pack lets you generate strong keys in your on-premises nShield HSM and securely export them to your cloud applications, whether you use Amazon Web Services, Google Cloud Platform, Microsoft Azure, or Salesforce. With BYOK, you strengthen the security of your key management practices, gain greater control over your keys, and ensure that you are sharing in the responsibility of keeping your data secure in the cloud.

BYOK with nShield HSMs brings you the following benefits:

- Safer key management practices that strengthen the security of your sensitive data in the cloud
- Stronger key generation using a high-entropy random number generator protected by FIPS-certified hardware
- Greater control over keys by using your own Shield HSMs in your own environment to create and securely export your keys to the cloud while retaining your own backup

Maximum control of your keys with Hold Your Own Key (HYOK)

Regulated industries typically have their options prescribed by security and data handling policies, government mandates (data sovereignty considerations for example), and the overall security posture of the organization. Data sovereignty has recently become a “hot potato” in the European Union, where the outcome of the Schrems II legal case led to more than 5,000 EU organizations having to think carefully about where their cryptographic keys and encrypted data reside. In response, cloud service provider AWS offers their Key Management Service External Key Store or AWS KMS XKS. It empowers organizations to own, hold, and manage their cryptographic keys on premises or in a cloud-based solution under their control, completely outside of the AWS ecosystem. nShield HSMs integrate seamlessly with AWS KMS XKS. In Microsoft Azure Information Protection (AIP) environments, nShield HSMs support Double Key Encryption designed to help enterprises protect their most sensitive content in Microsoft 365.

Streamlined operations using remote management

nShield Remote Administration, available for nShield network-attached and PCIe HSMs, helps you:

- Cut operational costs while staying informed and in command of your HSM estates 24x7
- Optimize HSM performance, infrastructure planning, and uptime using nShield Monitor to inform your staff about load trends, usage statistics, tamper events, warnings, and alerts
- Reduce travel costs and save time by easily managing HSMs through a powerful and secure interface

Remote configuration

nShield network-attached models offer a serial console option simplifying the physical installation of the HSM to racking, cabling, and applying power. All other HSM and network configuration can then be done remotely. This makes for easy deployment and redeployment without the need to revisit the data center. This feature supports a provider/tenant model where the provider controls the network configuration and the tenant has full control of their key material.

Highly flexible Security World Architecture

nShield Security World Architecture supports nShield HSMs by creating a unique, flexible key management environment. It lets you combine different nShield HSM models to build a unified ecosystem that delivers scalability, seamless failover, and load balancing. It also provides interoperability whether you deploy one or hundreds of HSMs, lets you manage an unlimited number of keys, and backs up and restores key material automatically and remotely.

nShield Security World Architecture offers the following benefits:

- Helps you easily scale your nShield HSM estate as your needs grow
- Preserves system resiliency
- Saves time by eliminating time-consuming HSM backups

Centralized remote management with KeySafe 5

Entrust KeySafe 5 offers the ability to centrally and remotely manage the setup and configuration to see the status of the scalable Security World architecture for mixed estates of nShield and nShield as a Service HSMs.

Secure execution environment

In addition to protecting your sensitive keys, nShield network-attached and PCIe HSMs also provide a secure environment for running your proprietary applications. The CodeSafe® software developer toolkit lets you develop and execute code within the nShield HSM's FIPS Level 3 physical boundary, safeguarding your applications from potential attacks.

The CodeSafe toolkit helps you:

- Achieve high assurance by executing sensitive applications and protecting application data endpoints inside a certified environment
- Protect security-sensitive applications against hazards, such as insider attacks, malware, and advanced persistent threats
- Eliminate the risk of unauthorized application changes or malware infection using code signing
- Deploy post-quantum algorithms such as LMS using the Post-Quantum Option Pack with CodeSafe software developer toolkit running inside the FIPS boundary of an nShield HSM

Support for crypto-agility

Crypto-agility is the capability of organizations to seamlessly adopt new, emerging encryption methods. This is critical as the first waves of post-quantum cryptographic algorithms are standardized, and as additional algorithms continue to be introduced.

The nShield 5 HSM offers crypto-agility out of the box with its security processor, a field-programmable gate array (FPGA) that can be readily reprogrammed via software updates. This reduces costly and time-consuming hardware refreshes and increases resilience against quantum computers that may compromise the encryption techniques we rely on today.

As we prepare for the coming challenge of quantum computers, HSMs are essential to the security and trust of IT systems, the cloud, and the internet. nShield 5 HSMs natively support NIST standardized PQC algorithms such as ML-DSA.

Partnering With Industry Leaders

Entrust partners with leading technology providers to deliver enhanced solutions that address a wide set of industry security challenges and help customers achieve their digital transformation goals. Through the Entrust Ready Technology Partner Program, we collaborate with partners to integrate nShield HSMs into a variety of security solutions, including:

- Credentialing and PKI
- Database security
- Code signing
- Digital signatures
- Privileged account management
- 5G
- Application delivery
- Cloud intelligence
- Big data intelligence

nShield HSMs support our partners' security applications to provide the strongest cryptographic processing, key protection, and key management available, while facilitating compliance with government and industry data security regulations.

> We are excited about the possibilities that nShield's new cloud-friendly features, including nShield as a Service, offer our customers. These new features recognize that the market is changing; that organizations need the capabilities of full-service HSMs in the cloud to unleash the innovation and commercial benefits available."
>
> **MATT LANDROCK, CORPORATE DIRECTOR, CRYPTOMATHIC**

> "The launch of nShield as a Service from Entrust gives F5 customers enhanced security choices with the ability to achieve data sovereignty on a subscription-based model. Shifting security from a capital to an operational expenditure enables greater flexibility and cost-effectiveness for organizations."
>
> **JOHN MORGAN, VP & GM OF SECURITY, F5 NETWORKS**

> "The Entrust nShield HSMs are state of the art and have therefore enabled us to use a more sophisticated and secure chip in our technology."
>
> **BILL KAVADAS, SENIOR DIRECTOR FOR INFORMATION SYSTEMS, MEMJET**

Versatility and High Performance

nShield network-attached and PCIe form-factor HSMs are available in three performance levels to suit your environment, whether your transaction rates are moderate or your application demands high throughput. nShield as a Service, our subscription-based solution for accessing nShield HSMs in the cloud, is underpinned by our highest performance network-attached HSMs.

nShield Root of Trust for Enterprise KMS

If your organization is seeking an enterprise key management service underpinned by an HSM root of trust, consider the Entrust Cryptographic Security Platform. Its key and secrets management solution redefines cryptographic key management by combining traditional key lifecycle management and a decentralized vault-based architecture with a comprehensive central policy and compliance management dashboard. This platform offers decentralized security with centralized visibility across the enterprise's cryptographic ecosystem – a powerful combination that helps ensure data is protected in line with stringent regulatory compliance mandates.

The Entrust Cryptographic Security Platform addresses the growing need for comprehensive cryptographic asset management in an increasingly complex digital landscape. It unifies cryptographic management by combining the rich capabilities to operate PKI, certificate lifecycle management, key management, and secrets management underpinned by an nShield HSM root of trust.

Certification to Industry Standards

Entrust's adherence to rigorous standards helps you demonstrate compliance in regulated environments while delivering high confidence in the security and integrity of nShield HSMs. Below is a partial list of the standards to which we comply. Complete lists are available on our website and in our data sheets.

FIPS 140-2/FIPS 140-3

Recognized globally, Federal Information Processing Standard (FIPS) 140-2 is a U.S. National Institute of Standards and Technology (NIST) certification that validates the security robustness of cryptographic modules. In 2022 this was superseded by the NIST FIPS 140-3 standard. nShield Solo XC and Connect XC HSMs have been certified to the established FIPS 140-2 standard. The nShield 5s and 5c have been certified to the newer FIPS 140-3 Level 3 standard.

FIPS 140-3 Validated,
Certificate #4745

Common Criteria and eIDAS compliance

nShield XC and nShield 5 HSMs are certified to Common Criteria EAL4+ and recognized as Qualified Signature Creation Devices (QSCDs) under the eIDAS Regulation. Our Common Criteria EAL4+ certified Entrust Remote QSCDs enable TSPs and signing system integrators (SIs) to offer eIDAS-certified remote signing services that are compliant with current eIDAS regulations. The Entrust Remote Type 2 QSCD combines the **Entrust Signature Activation Module (SAM)** with the **Entrust Solo XC HSM** to establish a root of trust required for highly secure and future-proof remote signature and seal services.

Additionally, nShield XC and nShield 5 HSMs are compliant with the Common Criteria Protection Profile EN 419 221-5 "Cryptographic Module for Trust Services." nShield HSMs are therefore able to serve as the security backbone for the digitalization of EU Member States and businesses. This includes enabling national ID schemes and crossborder services, qualified services for electronic documents and transaction signing, plus services for authentication, timestamping, secure email, and long-term document preservation. These certifications were established as part of European regulation and continue to be adopted by many countries around the globe.

For more information

Visit **entrust.com/HSM** to learn how we can protect your business-critical information and applications on your own premises, in the cloud, and in virtual 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 www.entrust.com.

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

ENTRUST
SECURING A WORLD IN MOTION