nShield® General Purpose Hardware Security Modules

ENTRUST

SECURING A WORLD IN MOTION

Contents

Security you can trust 3
The nShield family 4
nShield Connect 4
nShield Edge 4
nShield Solo 4
nShield as a Service 4
Support for a wide variety of uses 5
Features of the nShield family 5
Cloud-friendly web service interfaces 5
Containerized support on premises or in the cloud 6
Stronger key management for your cloud data with nShield BYOK 6
Streamlined operations using remote monitoring and management 7
Remote configuration 7
Security World's highly flexible architecture 7
CodeSafe - nShield's secure execution environment 8
Partnering with industry leaders 9
Versatility and high performance 10
Certification to industry standards 10
FIPS 140-2 10
Common Criteria and eIDAS compliance 11

Security you can trust

Entrust's nShield hardware security modules (HSMs) are hardened, tamper-resistant devices that protect your company's most sensitive data. These FIPS 140-2 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 to:

- Achieve higher levels of data security and trust
- Meet and exceed important regulatory standards
- Maintain high service levels and business agility

The nShield family

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

nShield Connect

Network-attached appliances

nShield Connect HSMs deliver cryptographic services to applications distributed across the network. nShield Connect HSMs are available in a range of feature rich nShield Connect XC models.

nShield Edge

Portable USB-based modules

nShield Edge HSMs are desktop devices designed for convenience and economy. nShield Edge is ideal for developers, and supports applications such as low volume root key generation.

nShield Solo

PCIe cards for embedding in appliances or servers

nShield Solo HSMs are low-profile PCI-Express card modules that deliver cryptographic services to applications hosted on a server or appliance. nShield Solo HSMs are available in a range of feature rich nShield Solo XC models.

nShield as a Service

Subscription-based solution for accessing nShield HSMs in the cloud

nShield as a Service provides access to dedicated FIPS 140-2 Level 3 certified nShield Connect XC HSMs via a subscription model. The solution delivers 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 maintenance of these appliances to the experts at Entrust. Available as self-managed and fully managed service options.

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, and blockchain. As growth in the Internet of Things 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 elliptic-curve cryptography algorithms that deliver high-speed transactions ideally suited to today's compact computing environments, as well as industry's most widely used operating systems and APIs.

Features of the nShield family

Cloud-friendly web service interfaces

The optional nShield Web Services Option Pack streamlines the interface between your applications and HSMs by executing commands through web service calls. This innovative approach simplifies deployments by removing the need to integrate applications directly with nShield, and eliminates dependencies on OS and architecture design choices. A cloud-friendly solution, the Web Services Option Pack interfaces with applications hosted in the cloud as well as in traditional data centers.

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 Entrust's high-assurance hardware security modules. 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 customers' applications and containerized hosts.

Stronger key management for your cloud data with nShield BYOK

nShield BYOK (Bring Your Own Key) 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 all three. nShield BYOK also supports exporting your keys to Salesforce. With nShield 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.

nShield BYOK brings you the following benefits:

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

For BYOK in Microsoft Azure, Amazon Web Services, Salesforce, and Google Cloud Platform, choose Entrust's Cloud Integration Option Pack (CIOP). The option pack contains all you need to use your on-premises nShield HSMs to generate and lease your keys to Microsoft Azure, Amazon Web Services, Salesforce, or Google Cloud Platform.

Streamlined operations using remote monitoring and management

nShield Monitor and nShield Remote Administration, available for nShield Solo and Connect HSMs, help you cut operational costs while staying informed and in command 24x7 of your HSM estates.

Entrust's remote monitoring and management offer the following benefits:

- 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 managing HSMs through nShield Remote Administration's powerful and secure interface

Remote configuration

nShield Connect XC 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.

Security World's highly flexible architecture

nShield Security World supports Entrust nShield HSMs by creating a unique, flexible key management environment. With nShield Security World, you can combine different nShield HSM models to build a unified ecosystem that delivers scalability, seamless failover, and load balancing.

"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

nShield Security World 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 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

CodeSafe - nShield's secure execution environment

In addition to protecting your sensitive keys, nShield Solo and Connect HSMs also provide a secure environment for running your proprietary applications. The CodeSafe option lets you develop and execute code within the nShield's FIPS 140-2 Level 3 boundaries, safeguarding your applications from potential attacks.

CodeSafe helps you to:

- 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

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 technology partner program, Entrust collaborates 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, application delivery, and cloud and 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

Versatility and high performance

nShield Connect and Solo 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 nShield Connect XC.

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

Recognized globally, FIPS 140-2 is a U.S. government NIST standard that validates the security robustness of cryptographic modules. All Entrust nShield HSMs are certified to FIPS 140-2 Level 2 and Level 3.

FIPS Level 3 Validated 140-2

Common Criteria

Common Criteria and eIDAS compliance

nShield XC HSMs are certified to Common Criteria EAL 4+ and recognized as qualified signature creation devices (QSCDs) under the eIDAS regulation. Additionally nShield Solo XC and Connect XC HSMs are compliant with the Common Criteria Protection Profile EN 419 221-5 "Cryptographic Modules 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 cross-border services, services for electronic documents and transaction signing, plus services for authentication, time stamping, secure email, and long-term document preservation. Although these certifications were established as part of a European regulation, they are being adopted by many countries around the globe.

For more information

Visit us at **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.

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com
entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

HS22Q1-entrust-nshield-family-br

ENTRUST

Contact us:
HSMinfo@entrust.com