THALES

www.thalesesecurity.com

‹Thales eSecurity›

nSHIELD® GENERAL PURPOSE HARDWARE SECURITY MODULES

Contents

Security you can trust

Thales eSecurity'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 two series: classic nShield Connect+ HSMs and the high-performance nShield Connect XC HSM series.

nSHIELD EDGE

portable USB-based modules
nShield Edge HSMs are desktop devices designed for convenience and economy. The 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 two series: classic nShield Solo+ HSMs and the high-performance nShield Solo XC HSM series.

Support for wide variety of uses

Thales customers use nShield HSMs as the root of trust in a variety of business applications including public key infrastructures (PKI), SSL/TLS 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.

"In order to create scalable, efficient and highly secure blockchain solutions, Accenture, a leader in blockchain solutions, is collaborating with Thales, the HSM gold standard."

John Velissarios, Security Principal Director, Accenture

Features of the nShield family

CLOUD-FRIENDLY WEB SERVICE INTERFACES

The optional nShield Web Services Crypto API streamlines the interface between your applications and HSMs by executing commands through web service calls. This innovative approach facilitates 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 Crypto API interfaces with applications hosted in the cloud as well as in traditional data centers.

STRONGER KEY MANAGEMENT FOR YOUR CLOUD DATA WITH nSHIELD BYOK

nShield BYOK 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. 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

"As a result of our collaboration with Thales, our customers can generate and upload their own master keys to a cloud-based HSM and keep complete control over their keys, giving them confidence that their data is protected."

Dan Plastina, Partner Group Program Manager, Microsoft

Microsoft Azure

amazon web services

Google Cloud Platform

STREAMLINED OPERATIONS USING REMOTE MONITORING AND MANAGEMENT

CipherTrust® 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.

Thales' remote monitoring and management products help you to:

- Optimize HSM performance, infrastructure planning and uptime using CipherTrust 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

SECURITY WORLD'S HIGHLY FLEXIBLE ARCHITECTURE

nShield HSMs are an integral part of the Thales Security World architecture which creates a unique, flexible key management environment. With Security World, you can combine different nShield HSM models to build a unified ecosystem that delivers scalability, seamless failover and load balancing.

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.

Thales 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 back-ups

"Thales's product has been an important component in delivering a service with exceptional levels of performance and scalability."

Steve Collins, Director, Emerging Markets Group, Barclays

CODESAFE - nSHIELD'S SECURE EXECUTION ENVIRONMENT

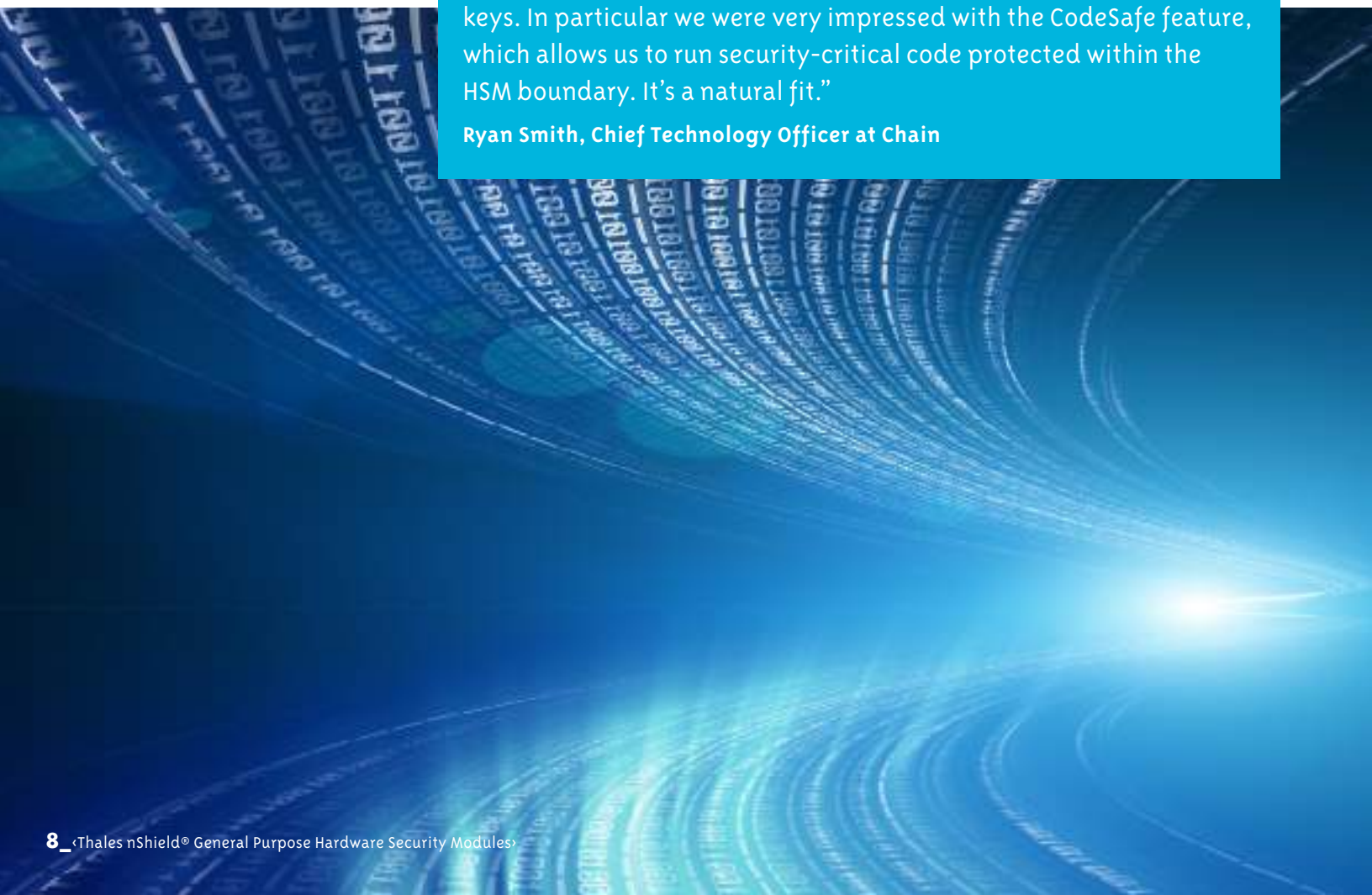
In addition to protecting your sensitive keys, nShield Solo and Connect HSMs also provide a secure environment for running your proprietary applications. The CodeSafe option lets you develop and execute code within the nShield's FIPS 140-2 Level 3 boundaries, safeguarding your applications from potential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

CodeSafe helps you to:

- Achieve high assurance by executing sensitive applications and protecting application data end points 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

"Thales nShield HSMs offer a fast and efficient way to derive new keys. In particular we were very impressed with the CodeSafe feature, which allows us to run security-critical code protected within the HSM boundary. It's a natural fit."

Ryan Smith, Chief Technology Officer at Chain



Partnering with industry leaders

Thales 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 Thales Alliance for Solutions and Application Provider (ASAP) program, Thales 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. Thales 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.

"F5's support for the Thales nShield HSMs provides the highest level of physical protection for cryptographic keys, enabling organizations to establish and prove compliance with the latest government legislation and security frameworks."

Siva Mandalam, Senior Director, Product Management, F5 Networks

"We provide managed service PKIs for a wide variety of organizations, and all of our managed PKI solutions rely on Thales HSMs because of their unique combination of strong security and operational ease for critical functions like key backup."

Robert Hann, Business Development Director, Trustis

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.

Certification to industry standards

Thales' 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 Thales nShield HSMs are certified to FIPS 140-2 Level 2 and Level 3 and are available for purchase at either level.

COMMON CRITERIA AND eIDAS COMPLIANCE

nShield Solo+ and Connect+ models are certified to Common Criteria (EAL) 4+ and are also recognized as qualified signature creation devices (QSCDs). As QSCDs, nShield HSMs are qualified to serve as the security backbone of European digital signature (eIDAS) and other globally recognized solutions including authentication services, digital signing and time stamping.

For more information

To learn more, please visit
www.thalesesecurity.com/products/general-purpose-hsms

THALES

www.thalesesecurity.com

About Thales e-Security

Thales e-Security is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales e-Security is part of Thales Group.

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thalesesecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thalesesecurity.com