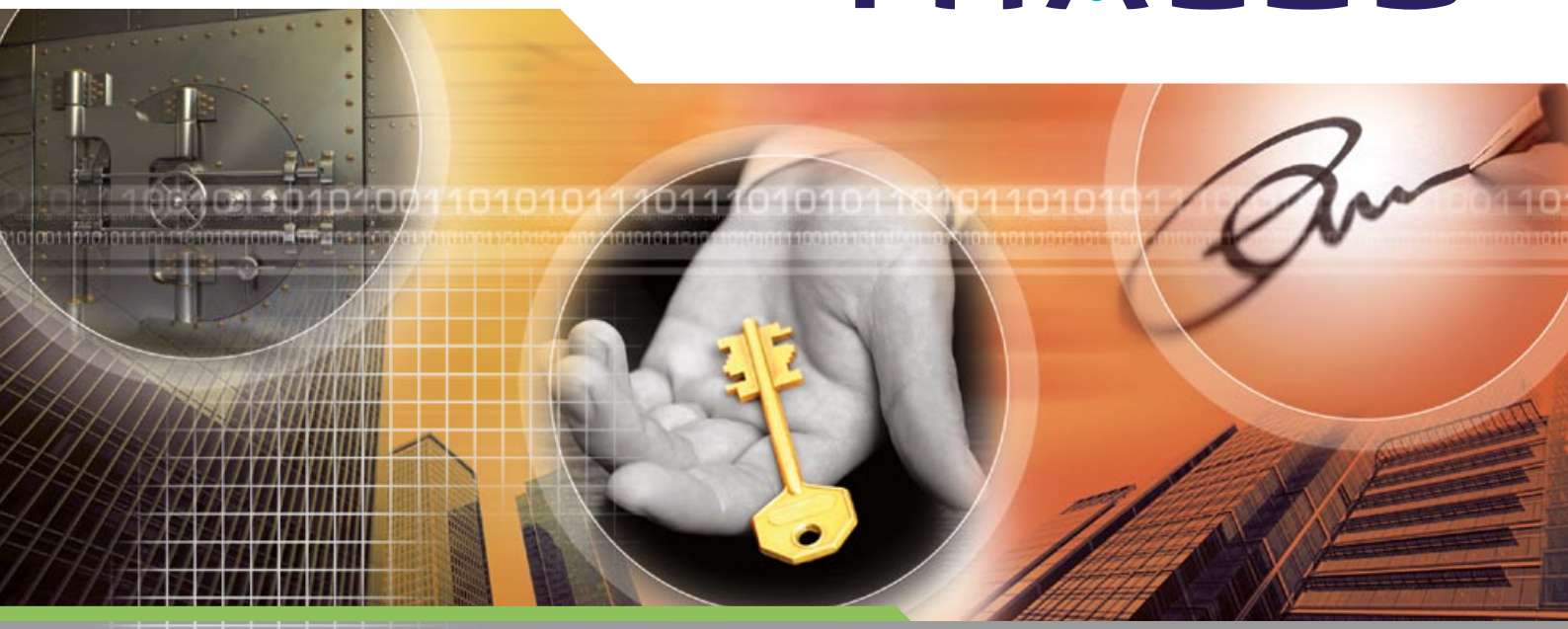
THALES



> Hardware Security Module

Thales nShield Solo

KEY BENEFITS

OPERATIONAL

- > Provides cost-effective cryptographic acceleration and unmatched operational flexibility in traditional data center and cloud environments leveraging unique Security World architecture
- > Reduces overall cost for regulatory compliance (e.g. PCI DSS) as well as for day-to-day key management tasks including backup and remote management
- > Enables high assurance business continuity with simplified HSM enrollment and efficient key provisioning
- > Enhances security and provides cryptographic acceleration for OEM appliances

Security

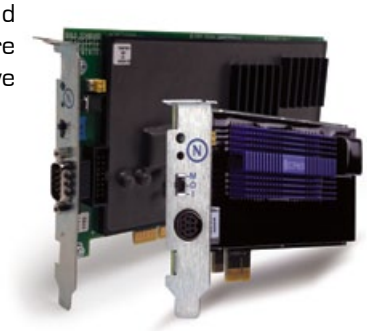
- > Delivers certified protection for cryptographic keys and operations within tamper-resistant hardware to significantly enhance security for critical applications
- > Establishes strong separation of duties and dual controls through robust administration policies including role-based multi-factor authentication and flexible quorum-based authorization
- > Enables secure execution of custom security-critical application code within the hardware security boundary

Microsoft GOLD CERTIFIED Partner ISV

ORACLE CERTIFIED PARTNER

The nShield Solo is the server-embedded hardware security module (HSM) in the Thales family of high security data protection solutions. The hardened cards, including a model optimized for elliptic curve cryptography, safeguard and manage sensitive keys used for encryption and digital signing on behalf of a wide range of commercial and custom-built business applications. nShield Solo protects critical security systems including public key infrastructures (PKIs), identity management, databases, web fabric, domain name system security extension (DNSSEC) deployments and code signing.

The nShield Solo provides cost-effective and dedicated physical and logical controls for server-based systems where software-based security features are considered to be inadequate. In the face of evolving compliance requirements and general standards of due care, the use of nShield HSMs provides a tangible measure of security within the traditional data center and cloud-based services. All Thales nShield HSMs feature the market-leading Security World key management architecture that enables the automation of burdensome and risk-prone administrative tasks, guarantees key recovery and eliminates single points of failure and expensive, manually-intensive backup processes.



> Thales nShield Solo

Technical Specifications*

Functional Capabilities

> Embedded one-to-one client server application support
> Onboard secure key and application storage/processing
> Cryptographic offloading/acceleration
> Authenticated multi level access control
> Strong separation of duties (administrator and operator)
> Secure key wrapping, backup, replication and recovery
> Unlimited protected key storage
> Clustering, load-balancing and "k of n" multifactor authentication
> Unlimited logical/cryptographic separation of application keys

Supported Operating Systems

> Physical: Windows, Linux, Solaris, IBM AIX, HP-UX

Application Program Interfaces (APIs)

> PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG
> nCore (low-level Thales interface for developers)

Compatibility and Upgradeability

> Compatible with Thales nShield Connect, nShield Edge and netHSM 500 and 2000
> Software upgradeable

Host Connectivity

> PCI 2.3 compliant; 2.1, 2.2, PCI-X compatible
> PCIe single lane compliant; 1.1, 2.0 compatible

Cryptography

> Asymmetric public key algorithms: RSA (1024, 2048, 4096), Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH
> Symmetric algorithms: AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, Triple DES
> Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512bit)
> Full Suite B implementation with fully licensed Elliptic Curve Cryptography (ECC) including Brainpool and custom curves

Safety, Security and Environmental Compliance

> UL, CE, FCC
> RoHS, WEEE
> FIPS 140-2 Level 2 and Level 3, NIST SP 800-131A**
> Common Criteria EAL4+**

High Availability

> All solid-state storage
> MTBF – Mil-Std 217F notice 2 parts count method (see table)

Management and Monitoring

> Remote unattended operator/multi-user access control
> Syslog diagnostics support
> Windows performance monitoring
> Command line interface (CLI)/graphical user interface (GUI)
> SNMPv3 compatible monitoring

Physical Characteristics

> Standard PCI and low profile PCIe form factor with external smart card reader
> Temperature: operating 10 to 35°C (50 to 95°F), storage -20 to 70°C (-4 to 158°F)
> Humidity: operating 10 to 90% (relative, non-condensing at 35%), storage 0 to 85% (relative, non-condensing at 35%)
> Dimensions, weight, max. power consumption, and MTBF:

Model No.	Dimensions (mm/in)	Weight (g/lbs)	Power (W)	MTBF (hrs)
PCI 500	107 x 129 x 15mm 4.2 x 5.1 x 0.6in	330g 0.7lb	14	193,000
PCIe 500, PCIe 6000	56.2 x 167.1 x 15.4mm 2.2 x 6.6 x 0.6in	230g 0.5lb	10	216,600
PCIe 6000+	56.2 x 167.1 x 15.4mm 2.2 x 6.6 x 0.6in	230g 0.5lb		
PCI 2000, PCI 4000	107 x 175 x 16.5mm 4.2 x 6.9 x 0.6in	340g 0.8lb	14	125,700

Cost-effective for Standalone Servers

When protecting cryptographic keys on standalone servers, nShield Solo is the most cost-effective solution. nShield Solo can be deployed within a cluster of servers to enable load balancing and high availability. For customers deploying multiple nShield Solo modules in a data center environment, an optional SmartCard Reader rackmount is available.

Optional nShield SmartCard Reader rackmount.

Available Models and Performance

nShield Solo is available in a variety of speeds and form factors:

Model	PCI 500	PCIe 500	PCI 2000	PCI 4000	PCIe 6000
Signing Performance RSA (tps)					
1024bit	500	500	2000	4000	6000
2048bit	80	150	300	580	3000
4096bit	15	65	20	40	500

Model	PCIe 6000+
Signing Performance ECC NISTP (tps)	
192bit	2300
256bit	2400
521bit	1300

For more information please see www.thales-esecurity.com or scan the quick response (QR) code on your smart phone.

* Performance may vary depending on operating system, application, network topology and other factors.

** Model 6000+ under FIPS and Common Criteria evaluation.

Americas: 900 South Pine Island Road, Suite 710, Plantation, Florida 33324 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.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@thales-esecurity.com