THALES

www.thales-esecurity.com

nSHIELD SOLO

- Maximize performance and availability with high cryptographic transaction rates and flexible scaling.
- Supports a wide variety of applications including certificate authorities, code signing and more.
- nShield CodeSafe protects your applications within nShield's secure execution environment.
- nShield Remote Administration helps you cut costs and reduce travel.

‹Thales e-Security›

nSHIELD SOLO HSMs

Certified PCI-Express Cards that Deliver Cryptographic Key Services to Stand-alone Servers

‹Thales e-Security›

nSHIELD SOLO HSMs

Feature Overview

nShield Solo hardware security modules (HSMs) are FIPS-certified, low-profile PCI-Express cards that deliver cryptographic services to applications hosted on a server or appliance. These tamper-resistant cards perform such functions as encryption, digital signing and key generation and protection over an extensive range of applications, including certificate authorities, code signing, custom software and more.

The nShield Solo series includes nShield Solo+ and the new, high-performance nShield Solo XC.

HIGHLY FLEXIBLE ARCHITECTURE

Thales's unique Security World architecture lets you combine nShield HSM models to build a mixed estate that delivers flexible scalability and seamless failover and load balancing.

PROCESS MORE DATA FASTER

nShield Solo HSMs support high transaction rates, making them ideal for enterprise, retail, IoT and other environments where throughput is critical.

PROTECT YOUR PROPRIETARY APPLICATIONS AND DATA

The CodeSafe option provides a secure environment for running sensitive applications within nShield boundaries.

CERTIFIED HARDWARE SOLUTIONS

Thales's broad set of certifications help you demonstrate compliance and meet stringent industry standards.

TECHNICAL SPECIFICATIONS

Supported Cryptographic Algorithms

- Asymmetric public key algorithms: RSA, Diffie-Hellman, ECMQV, DSA, KCDSA, ECDSA, ECDH
- 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

Supported Operating Systems

- Windows and Linux
- Solo+ additionally supports Solaris, IBM AIX, HP-UX and virtual environment AIX LPARs
- Solo XC also supports virtual environments Citrix XenServer 6.5, VMware ESXi 5.5, and Windows Server 2012R2 Hyper-V

Application Programming Interfaces (APIs)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG nCore

Host Connectivity

- PCI Express Version 2.0; Solo+ connector: 1 lane, Solo XC connector: 4 lane

Security Compliance

- FIPS 140-2 Level 2 and Level 3 for Solo+; Solo XC is FIPS-pending
- USvG6 accreditation for Solo+ and Solo XC
- Common Criteria EAL4+ (AVA_VAN.5) for Solo+
- Recognition of Solo+ as a Qualified Signature Creation Device

Safety and Environmental Standards Compliance

- UL, UL/CA, CE, FCC, Canada ICES, KC, FCC, VCCI, C-TICK, RCM
- RoHS2, WEEE, REACH

Management and Monitoring

- Cut costs using nShield Remote Administration. Please consult the nShield Remote Administration data sheet to learn more.
- Syslog diagnostics support Windows performance monitoring
- SNMP monitoring agent

Dimensions	Weight		Power	
	Solo+	Solo XC	Solo+	Solo XC
56.2 × 167.1 × 15.4mm	230g	280g	10W	24W
2.2 × 6.6 × 0.6in	0.5lb	0.62lb		

Available Models and Performance

nShield Solo Models	500+	XC Base	6000+	XC Mid	XC High
RSA Signing Performance (tps) for NIST Recommended Key Lengths					
2048 bit	150	430	3,000	3,500	8,600
4096 bit	80	100	500	850	2,025
ECC Prime Curve Signing Performance (tps) for NIST Recommended Key Lengths					
256 bit	540	680	2,400	5,500	16,000

LEARN MORE

Visit us at www.thales-esecurity.com to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

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@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