

## 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 eSecurity»

## nSHIELD SOLO HSMs

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



# 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.

### Supported Cryptographic Algorithms

- > Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- > Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD 160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, Triple DES
- > Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD 160
- > Full Suite B implementation with fully licensed ECC, including Brainpool and custom curves

### Supported Operating Systems

- > Microsoft Windows 7 x64, 10 x64; Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- > Red Hat Enterprise Linux AS/ES 6 x64, 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
- > Oracle Solaris 11 (SPARC), Oracle Solaris 11 x64
- > Solo+: Red Hat Enterprise Linux AS/ES 6 x86, IBM AIX 7.1 (POWER6), HP-UX 11i v3
- > Oracle Enterprise Linux 6.8 x64 and 7.1 x64
- > Solo XC virtual environment support: Microsoft Windows Hyper-V Server 2016, VMware ESXi 6.5, Citrix XenServer 6.5

Follow us on:



### Application Programming Interfaces (APIs)

- > PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore, nShield Web Services Crypto API

### 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 certified
- > Solo+: Common Criteria EAL4+ (AVA\_VAN.5) certified
- > Solo+ recognized as a Qualified Signature Creation Device
- > Solo XC: BSI AIS 20/31 compliant

### Safety and Environmental Standards Compliance

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

### Management and Monitoring

- > nShield Remote Administration and CipherTrust Monitor
- > Secure audit logging
- > Syslog diagnostics support and 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	14,400

### LEARN MORE

Visit us at [www.thalesecurity.com](http://www.thalesecurity.com) to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.