THALES

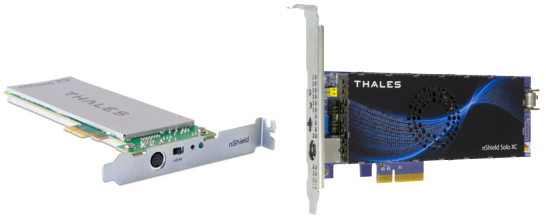
www.thales-esecurity.com

SERVER-EMBEDDED HARDWARE SECURITY MODULES

The Thales nShield Solo series are embedded hardware security modules (HSMs) that increase the digital security of an organization's critical business applications by isolating sensitive tasks, securely executing cryptographic operations, and protecting and managing the associated keys. These hardened, tamper-resistant PCIe cards performs encryption, digital signing, and key management on behalf of an extensive range of commercial and custom-built applications including public key infrastructures (PKIs), identity management systems, application-level encryption and tokenization, SSL/TLS, and code signing. High assurance alternatives to software-based cryptography libraries, nShield Solo modules feature certified implementations of all leading algorithms including Suite B, as well as best in class elliptic curve cryptography (ECC) performance.

Key Benefits

- Automate risk-prone administrative tasks, guarantee key recovery, and eliminate costly manually-intensive backup processes
- Remote Administration feature reduces the cost of traveling to data centers
- Establish strong separation of duties through robust administration policies including roles-based multi-factor authentication and quorum-based authorization
- Enable secure execution of custom security-critical application code within the tamper-resistant hardware boundary



Thales e-Security

nShield Solo Series

Solo+ and Solo XC

Thales nShield Solo Series

TECHNICAL SPECIFICATIONS[1]

Functional capabilities

- Embedded one-to-one client server application support
- Secure key and application storage and processing
- Cryptographic offloading and acceleration
- Authenticated multi level access control
- Strong separation of administration and operator roles
- Secure key wrapping, backup, replication and recovery
- Unlimited protected key storage
- Supports clustering and load-balancing
- Logical cryptographic separation of application keys
- "k of n" multi-factor authentication

Supported operating systems

- Windows, Linux, Solaris[4], IBM AIX[4], HP – UX[4]
- Remote Administration client side: Windows, Linux

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/Connect+, nShield Solo PCI/PCIe and nShield Edge
- Security World key management architecture enables load balancing across mixed estates of nShield models
- Software upgradeable

Host connectivity

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

Cryptography

- Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA[3], ECDH[3]
- Symmetric algorithms: AES, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, Triple DES
- Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit)
- Full Suite B implementation with fully licensed ECC including Brainpool and custom curves

Security[2] compliance

- FIPS 140-2 Level 2 and Level 3 (XC models FIPS-pending)

Safety and environmental compliance

- UL, UL/CA[5], CE, FCC, Canada ICES, KC, FCC, VCCI, C-TICK[4], RCM[5]
- RoHS2, WEEE, REACH

Management and monitoring

- Remote Administration enables management – including adding applications, updating firmware, and checking nShield status – from your office location
- Syslog diagnostics support
- Windows performance monitoring
- Command line interface (CLI)/graphical user interface (GUI)
- SNMP monitoring agent

Physical characteristics

- Standard low profile PCIe form factor

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

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 Smart Card Reader rackmount is available.

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	340	3,000	3,000	8,400
4096 bit	80	80	500	700	2,000
ECC Prime Curve Signing Performance (tps) for NIST Recommended Key Lengths[3]					
256 bit	540	570	2,400	5,000	14,000

Microsoft Partner
Gold Application Development

1 Performance may vary depending on operating system, application, network topology and other factors.
2 Security certifications are performed only against select firmware versions. Consult the certifications section of our website for links to official certificates.
3 With ECC Activation
4 Solo+ models only
5 Solo XC models only

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