THALES

www.thales-esecurity.com

SERVER-EMBEDDED HARDWARE SECURITY MODULE

The Thales nShield Solo+ is a hardware security module (HSM) that isolates and secures cryptographic operations and associated keys for an organization's most critical applications. This hardened, tamper-resistant PCIe card 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. A high assurance alternative to software-based cryptography libraries, nShield Solo+ features certified implementations of all leading algorithms, as well as the world's fastest ECC performance.

Key Benefits

- Automates burdensome and risk-prone administrative tasks, guarantees key recovery, and eliminates single points of failure and expensive, manually-intensive backup processes
- 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 tamper-resistant hardware boundary

Thales e-Security

nShield Solo+

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/Connect+, nShield Solo PCI/PCIe and nShield Edge
- Software upgradeable

Host connectivity
- PCIe single lane compliant; 1.1, 2.0 compatible

Cryptography
- A symmetric 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, 512 bit)
- 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

High availability
- 216,600 hrs MTBF (Mil-Std 217F notice 2 parts count method)

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 low profile PCIe form factor with optional external Smart Card Reader rackmount
- 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%)

Model	Dimensions (mm/in)	Weight (g/lbs)	Power (W)
PCIe 500+	56.2 x 167.1 x 15.4mm	230g	10
PCIe 6000+	2.2 x 6.6 x 0.6in	0.5lb	

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

Model	500+	6000+
RSA Signing Performance (tps) for NIST Recommended Key Lengths		
2048 bit	150	3000
4096 bit	80	500
ECC Prime Curve Signing Performance (tps) for NIST Recommended Key Lengths[Δ]		
192 bit	880	2300
256 bit	540	2400
521 bit	120	1300
ECC Key Generation Performance (keys/sec) for NIST Recommended Key Lengths[Δ]		
192 bit	400	830
256 bit	250	880
521 bit	60	600

[Δ]With ECC Activation

500+ model is available starting July 1, 2014.

Microsoft Partner
Gold Application Development

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

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 – 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