



> Thales nShield Solo

KEY BENEFITS

- > Cost-effective, dedicated HSM for servers
- > Protects cryptographic keys and data of sensitive applications in secure hardware
- > Enables easy automated key backup with secure recovery
- > Enhances security and cryptographic acceleration for OEM appliances
- > Reduces cost through remote management
- > Lowers TCO with Security World management
- > Avoids bottlenecks through premium performance
- > Readily integrates with third-party applications
- > Protects data in hostile environments with CodeSafe technology
- > Delivers FIPS and Common Criteria compliance

Embedded hardware security module for application key management

Thales nShield Solo, part of the nCipher product range, is a family of embedded, general-purpose HSMs for servers and appliances that safeguard encryption and digital signing keys and that can optionally run custom applications on the module to protect data in use. Previously known simply as "nShield", nShield Solo protects encryption and signing keys on servers in a highly secure, tamper-resistant hardware module. It is compatible with platforms offering PCI, PCI-X and PCI Express interfaces.



>> Thales nShield Solo

Hardware security for applications

nShield Solo enables enterprises to add hardware protection to critical applications such as public key infrastructures (PKIs), databases, web and application servers. nShield Solo modules are available as tamper-resistant PCI and PCI Express expansion cards; the PCI variant is also compatible with PCI-X interfaces.

Cost-effective for stand-alone servers

When protecting cryptographic keys on one or few stand-alone servers, nShield Solo is the most cost-effective solution. For customers deploying one or more nShield Solo modules in a 19" rack, the optional nShield SmartCard Reader Rackmount provides a practical and tidy solution to attach card readers in the data center.



Security and acceleration for OEM appliances

Hardware vendors can benefit from enhanced security for their appliances by using nShield Solo, which delivers FIPS and Common Criteria compliance for their key management. They also take advantage of performance increases for cryptographic operations.

Remote management and business continuity

In situations where nShield HSMs are deployed at a remote site or in a lights-out data center, Remote Operator can be used with an nShield Solo card in the operator's machine to remotely provide credentials. This accelerates security administration and reduces travel costs. nShield Solo can be deployed with clustered servers to enable load balancing and high availability.

Security World management lowers TCO

The Security World management software enables central management of nShield Solo, nShield Connect and netHSM to reduce setup and administration time. Security World enables remote operation of HSMs in lights-out data centers, disaster recovery even for total hardware replacements, and key sharing across HSMs and geographies. Keys and meta information can be automatically backed up without requiring additional hardware or on-site presence, reducing the total cost of operations.

Premium performance avoids bottlenecks

nShield Solo offers hardware acceleration for cryptographic operations of up to 6,000 signing transactions per second (TPS) with 1,024 RSA keys. Using RSA 2,048 bit keys, nShield Solo excels with up to 3,100 TPS.

Readily integrates with third-party applications

nShield Solo integrates with applications through standard interfaces including PKCS#11, Java Cryptography Extension (JCE), Microsoft CAPI and CNG. It is compatible with nShield Connect and can be upgraded to support additional features using various option packs. nShield Solo supports a broad range of operating systems, including Windows 2008/2003/Vista/XP, Linux Solaris, AIX and HP-UX.

Protects data in hostile environments

Most HSMs protect keys but not the data. Trojans or rogue administrators still have access to sensitive information on the host system. CodeSafe technology processes data inside the HSM instead of the host, enabling you to run critical processes in hostile environments.

Delivers FIPS and Common Criteria

nShield Solo supports a broad range of public-key and symmetric algorithms, including a full Suite B implementation with optional, fully licensed elliptic curve cryptography (ECC). nShield Solo's security boundary is validated to FIPS 140-2 Level 3 and Common Criteria EAL 4+. nShield Solo modules are also available with FIPS 140-2 Level 2 at a lower price. It separates administrative and operational duties with two-factor authentication and dual control. These operator groups can segregate access to keys by application, role, division, or geography.

For more information, please see www.thalesgroup.com/iss.

Thales - Information Systems Security

