



**ENTRUST**

## Entrust nShield® Solo HSMs

Certified PCI-Express cards that deliver cryptographic key services to stand-alone servers

### HIGHLIGHTS

Entrust 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.

### Highly flexible architecture

The nShield 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

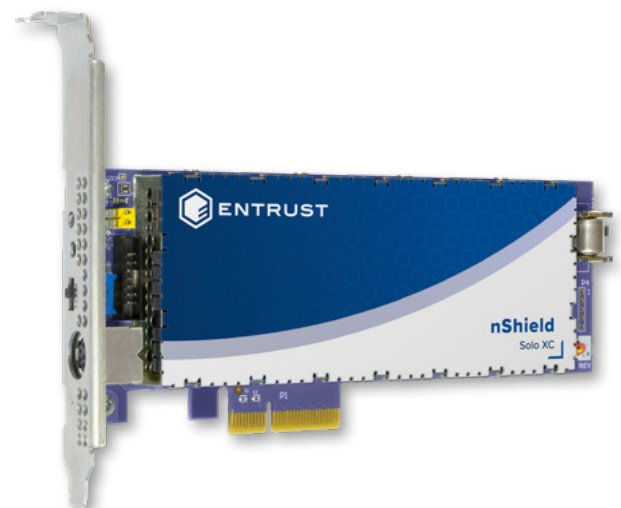
nShield Solo HSMs support high transaction rates, making them ideal for enterprise, retail, IoT and other environments where throughput is critical.

### Protect your proprietary applications and data

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

### KEY FEATURES & BENEFITS

- 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 option helps you cut costs and reduce travel



**LEARN MORE AT [ENTRUST.COM/HSM](https://www.entrust.com/hsm)**



# nShield Solo HSMs

## TECHNICAL SPECIFICATIONS

Supported cryptographic algorithms	Supported platforms	Application programming interfaces (APIs)
<ul style="list-style-type: none"> <li>Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)</li> <li>Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, 3DES</li> <li>Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160</li> <li>Full Suite B implementation with fully licensed ECC, including Brainpool and custom curves</li> <li>Elliptic Curve Key Agreement (ECKA) available via Java API and nCore APIs Elliptic Curve Integrated Encryption Scheme (ECIES) available via Java API, PKCS#11 and nCore APIs</li> </ul>	<ul style="list-style-type: none"> <li>Windows and Linux operating systems including distributions from RedHat, SUSE and major cloud service providers running as virtual machines or in containers</li> <li>Solo XC virtual environments supported including VMware ESX, Microsoft Hyper-V, Linux KVM &amp; Citrix XenServer</li> </ul>	<ul style="list-style-type: none"> <li>PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore, and Web Services (requires nShield Web Services Option Pack)</li> </ul>

Host connectivity	Security compliance	Safety and environmental standards compliance	Management and monitoring
<ul style="list-style-type: none"> <li>PCI Express Version 2.0; Solo XC connector: 4 lane</li> </ul>	<ul style="list-style-type: none"> <li>FIPS 140-2 Level 2 and Level 3 certified</li> <li>Solo XC recognized as a Qualified Signature Creation Device</li> <li>Solo XC: eIDAS and Common Criteria EAL4 + AVA_VAN.5 and ALC_FLR.2 certification against EN 419 221-5 Protection Profile, under the Dutch NSCIB scheme</li> <li>Solo XC: BSI AIS 20/31 compliant</li> </ul>	<ul style="list-style-type: none"> <li>UL, UL/CA, CE, FCC, Canada ICES, KC, FCC, VCCI, RCM</li> <li>RoHS2, WEEE, REACH</li> </ul>	<ul style="list-style-type: none"> <li>nShield Remote Administration and nShield Monitor</li> <li>Secure audit logging</li> <li>Syslog diagnostics support and Windows performance monitoring</li> <li>SNMP monitoring agent</li> </ul>

## AVAILABLE MODELS AND PERFORMANCE

nShield Connect models	XC Base	XC Mid	XC High
<b>RSA signing performance (tps) for NIST recommended key lengths</b>			
2048 bit	430	3,500	8,600
4096 bit	100	850	2,025
<b>ECC prime curve signing performance (tps) for NIST recommended key lengths</b>			
256 bit	680	7,515 <sup>2</sup>	14,400 <sup>2</sup>
<b>Symmetric encryption (KB/sec) 1024 byte plain text</b>			
3 DES 168 bit	685	5,140	5,500
AES 128 bit	825	7,700	11,300
<b>Key generation with ECC activation (keys/sec)</b>			
RSA 2048 bit	6.0	6.2	7.3
ECDSA P-192 bit	110	650	1,050
ECDSA P-256 bit	100	630	1,050
ECDSA P-521 bit	65	480	710

Each nShield Solo XC is supplied with an external smartcard reader and six smart cards for local use

LEARN MORE AT [ENTRUST.COM/HSM](http://ENTRUST.COM/HSM)

To find out more about  
Entrust nShield HSMs  
[HSMinfo@entrust.com](mailto:HSMinfo@entrust.com)  
[entrust.com/HSM](https://entrust.com/HSM)

## ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at  
[entrust.com](https://entrust.com)



Global Headquarters  
1187 Park Place, Minneapolis, MN 55379  
U.S. Toll-Free Phone: 888 690 2424  
International Phone: +1 952 933 1223  
[info@entrust.com](mailto:info@entrust.com) [entrust.com/contact](https://entrust.com/contact)

Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer. ©2022 Entrust Corporation. All rights reserved. HS22Q1-entrust-nshield-solo-ds