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
nShield Solo HSMs

TECHNICAL SPECIFICATIONS

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, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, 3DES
- Hash/message digest: MD5, SHA, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160
- Full Suite B implementation with fully licensed ECC, including Brainpool and custom curves
- 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

Supported platforms
- Windows and Linux operating systems including distributions from RedHat, SUSE and major cloud service providers running as virtual machines or in containers
- Solo XC virtual environments supported including VMware ESX, Microsoft Hyper-V, Linux KVM & Citrix XenServer

Application programming interfaces (APIs)
- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore, and Web Services (requires nShield Web Services Option Pack)

Host connectivity
- PCI Express Version 2.0; Solo XC connector: 4 lane

Security compliance
- FIPS 140-2 Level 2 and Level 3 certified
- Solo XC recognized as a Qualified Signature Creation Device
- 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 NCSIC scheme
- Solo XC: BSI AIS 20/31 compliant

Safety and environmental standards compliance
- UL, UL/CA, CE, FCC, Canada ICES, KC, FCC, VCCI, RCM
- RoHS2, WEEE, REACH

Management and monitoring
- nShield Remote Administration and nShield Monitor
- Secure audit logging
- Syslog diagnostics support and Windows performance monitoring
- SNMP monitoring agent

AVAILABLE MODELS AND PERFORMANCE

<table>
<thead>
<tr>
<th>nShield Connect models</th>
<th>XC Base</th>
<th>XC Mid</th>
<th>XC High</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA signing performance (tps) for NIST recommended key lengths</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2048 bit</td>
<td>430</td>
<td>3,500</td>
<td>8,600</td>
</tr>
<tr>
<td>4096 bit</td>
<td>100</td>
<td>850</td>
<td>2,025</td>
</tr>
<tr>
<td>ECC prime curve signing performance (tps) for NIST recommended key lengths</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>256 bit</td>
<td>680</td>
<td>7,515²</td>
<td>14,400²</td>
</tr>
<tr>
<td>Symmetric encryption (KB/sec) 1024 byte plain text</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 DES 168 bit</td>
<td>685</td>
<td>5,140</td>
<td>5,500</td>
</tr>
<tr>
<td>AES 128 bit</td>
<td>825</td>
<td>7,700</td>
<td>11,300</td>
</tr>
<tr>
<td>Key generation with ECC activation (keys/sec)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA 2048 bit</td>
<td>6.0</td>
<td>6.2</td>
<td>7.3</td>
</tr>
<tr>
<td>ECDSA P-192 bit</td>
<td>110</td>
<td>650</td>
<td>1,050</td>
</tr>
<tr>
<td>ECDSA P-256 bit</td>
<td>100</td>
<td>630</td>
<td>1,050</td>
</tr>
<tr>
<td>ECDSA P-521 bit</td>
<td>65</td>
<td>480</td>
<td>710</td>
</tr>
</tbody>
</table>

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

LEARN MORE AT 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.