Entrust nShield® 5s HSMs

High-performance, next-generation, crypto-agile PCI-express hardware security modules

HIGHLIGHTS

Comprehensive capabilities

Entrust nShield® 5s hardware security modules (HSMs) are FIPS 140-3 Level 3 (pending) low-profile PCI Express cards that deliver cryptographic services to applications hosted on a server or appliance.

- Maximize performance and availability with high cryptographic transaction rates and flexible scaling
- Supports a wide variety of applications including certificate authorities, code signing, 5G, and more
- FIPS 140-3 certification (in review)
- nShield Remote Administration option helps you cut costs and reduce travel
- Designed for multi-tenancy support

nShield 5s HSMs are tamper-resistant devices that perform functions such as encryption, digital signing, and key generation supporting a range of applications and technologies, such as:

- Certificate authorities
- Code signing
- Custom software
- Cloud and containerized applications
- Web services
- Remote signing
- Blockchain
- Database encryption
- 5G for telco environments
- IoT applications
- Car2X

Learn more at entrust.com/HSM
nShield 5s HSMs

KEY FEATURES & BENEFITS

Highly flexible architecture
nShield 5s is the latest addition to the range of HSMs that fit seamlessly with Entrust’s unique Security World architecture. Entrust Security World 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 5s HSMs support high transaction rates, making them ideal for application environments where throughput is critical, such as 5G, Car2X, and smart meters.

Centralized remote management
KeySafe 5, available with Security World software, allows organizations to centrally manage their estate of HSMs and associated Security Worlds remotely.

POWERFUL NSHIELD 5 REMOTE OPTIONS

Eliminate visits to the data center
nShield Remote Administration – Enables the secure remote presentation of authorization smart cards to remote HSMs to execute maintenance tasks including enrolling new HSMs and reassigning/reconfiguring existing HSMs. Separate data sheet available.

Remote Configuration – Serial console allows simple installation for data center staff, and allows HSM and client configuration without requiring physical access to the HSM front panel and front panel settings.

nShield Monitor – Provides a single dashboard of all your nShield HSMs, helping you to optimize operations and increase uptime. Separate data sheet available.

AVAILABLE MODELS AND PERFORMANCE

<table>
<thead>
<tr>
<th>nShield 5s models</th>
<th>Base</th>
<th>Mid</th>
<th>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>670</td>
<td>3,949</td>
<td>13,614</td>
</tr>
<tr>
<td>4096 bit</td>
<td>135</td>
<td>814</td>
<td>2,200</td>
</tr>
<tr>
<td>8192 bit</td>
<td>19</td>
<td>115</td>
<td>309</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>2,085</td>
<td>7,553</td>
<td>21,826</td>
</tr>
<tr>
<td>512 bit</td>
<td>1010</td>
<td>5,977</td>
<td>16,164</td>
</tr>
<tr>
<td>Key generation (keys/sec)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA 2048 bit</td>
<td>7</td>
<td>20</td>
<td>23</td>
</tr>
<tr>
<td>ECDSA P-256 bit</td>
<td>1,040</td>
<td>3,580</td>
<td>3,494</td>
</tr>
<tr>
<td>ECDSA P-521 bit</td>
<td>518</td>
<td>2,480</td>
<td>2,724</td>
</tr>
<tr>
<td>Key agreement performance (transactions/sec)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDSA P-256 bit</td>
<td>2,085</td>
<td>7,550</td>
<td>21,436</td>
</tr>
</tbody>
</table>

Each nShield 5s HSM is supplied with an external smart card reader for local use.
## TECHNICAL SPECIFICATIONS

### Supported cryptographic algorithms

- Full NIST Suite B implementation
- Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, ElGamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- Symmetric algorithms: AES, Arcfour, ARIA, Camellia, MDS 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-1, SHA-224, SHA-256, SHA-384, SHA-512, Tiger, 3DES
- 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
- TUAK and MILENAGE algorithm support for mutual authentication and key generation (3GPP)
- NIST short-listed post-quantum cryptographic algorithms supported using the nShield Post Quantum SDK with CodeSafe

### Supported platforms

- Windows and Linux operating systems including distributions from Red Hat, SUSE

### Application programming interfaces (APIs)

- PKCS#11
- OpenSSL
- Java (JCE)
- Microsoft CAPI/CNG
- Web Services
- nCore

### Host connectivity

- PCI Express Version 2.0; connector: 4 lane
- FIPS 140-3 Level 3 (pending)
- BSI AIS 20/31 compliant

### Security compliance

- UL, UL/CA, CE, FCC, Canada ICES, KC, VCCI, RCM, UKCA
- RoHS, WEEE, REACH

### Safety and environmental standards compliance

- KeySafe 5, nShield Remote Administration and nShield Monitor
- Secure audit logging
- Syslog diagnostics support and Windows performance monitoring
- SNMP monitoring agent

### Management and monitoring

- Dimensions: 167.7mm x 68.9mm (excludes mounting bracket dimensions)
- Weight: 270g
- Power: 25W
- Reliability – MTBF: 1,702,841 hours
- Mounting bracket – supplied with low profile (fitted) and full height bracket

---

**Note 1:** Calculated at 25 degrees centigrade operating temperature using Telcordia SR-332 “Reliability Prediction Procedure for Electronic Equipment” MTBF Standard

---

Learn more at entrust.com/HSM
ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it’s no wonder the world’s most entrusted organizations trust us.