



**ENTRUST**

## nShield Connect HSMs

The security of your applications depends on where you keep your keys

### HIGHLIGHTS

#### Comprehensive capabilities

nShield Connect hardware security modules (HSMs) are FIPS 140-2 and Common Criteria EAL4+ (EN 419 221-5) certified appliances that deliver scalable and highly available cryptographic key services across networks.

- High cryptographic transaction rates and flexible scaling
- Integrate with over 150 leading application provider solutions
- CodeSafe option for protecting your application and business logic within the nShield's secure execution environment

nShield Connect HSMs are tamper-resistant platforms that perform such functions as encryption, digital signing, and key generation and protection over a range of applications, such as:

- Certificate authorities
- Code signing
- Custom software
- Cloud and containerized applications
- Web Services
- Blockchain
- Database encryption

The nShield Connect series includes nShield Connect+ and the high-performance nShield Connect XC.



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



# nShield Connect HSMs

## KEY FEATURES & BENEFITS

### Highly flexible architecture

Our 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 Connect HSMs support high transaction rates, making them ideal for environments where throughput is critical, such as enterprise, retail and IoT.

## POWERFUL REMOTE FEATURE 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 firmware upgrades, enrolling new HSMs and reassigning/reconfiguring existing HSMs. Separate datasheet available.

Remote Configuration - Serial console version of Connect XC allows simple installation for data center staff, remote network configuration and front panel settings.

nShield Monitor provides a single dashboard of all your nShield HSMs helping you to optimize operations and increase uptime. Separate datasheet available.

### Protect your proprietary applications

The CodeSafe option provides a secure environment for running sensitive applications within nShield FIPS 140-2 physical boundary. Reference the CodeSafe datasheet for more detailed information.

## AVAILABLE MODELS AND PERFORMANCE

nShield Connect models	500+	XC Base	1500+	6000+	XC Mid	XC High
RSA signing performance (tps) for NIST recommended key lengths						
2048 bit	150	430	450	3,000	3,500	8,600
4096 bit	80	100	190	500	850	2,025
ECC prime curve signing performance (tps) for NIST recommended key lengths						
256 bit	540	680	1,260	2,400	7,515 <sup>2</sup>	14,400 <sup>2</sup>
Client licenses						
Included	3	3	3	3	3	3
Maximum	10	10	20	unlimited <sup>1</sup>	20	unlimited <sup>1</sup>

Note 1: requires enterprise client license.

Note 2: Performance indicated requires ECDSA fast RNG feature activation available free of charge on request from nCipher Support.



# nShield Connect HSMs

## TECHNICAL SPECIFICATIONS

Supported cryptographic algorithms (including full NIST Suite B implementation)	Supported platforms	Application programming interfaces (APIs)	Host connectivity	Security compliance
<ul style="list-style-type: none"> <li>Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (including NIST, Brainpool &amp; secp256k1 curves), ECDH, Edwards (Ed25519, Ed25519ph)</li> <li>Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, DES, 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> </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> </ul>	<ul style="list-style-type: none"> <li>PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG and Web Services (requires Web Services Option Pack)</li> </ul>	<ul style="list-style-type: none"> <li>Dual Gigabit Ethernet ports (two network segments)</li> </ul>	<ul style="list-style-type: none"> <li>FIPS 140-2 Level 2 and Level 3 certified</li> <li>IPv6 certified and USGv6 Ready compliant</li> <li>Connect 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>Connect+: Common Criteria EAL4+ (AVA_VAN.5) certified</li> <li>Connect+: Recognized as a Qualified Signature Creation Device</li> <li>Connect XC: BSI AIS 20/31 compliant</li> </ul>

Safety and environmental standards compliance	High availability	Management and monitoring	Physical characteristics
<ul style="list-style-type: none"> <li>UL, CE, FCC, RCM Canada ICES RoHS2, WEEE</li> </ul>	<ul style="list-style-type: none"> <li>All solid-state storage</li> <li>Field serviceable fan tray, dual hot-swap power supplies</li> </ul>	<ul style="list-style-type: none"> <li>nShield Remote Configuration (available on Serial Console-configured Connect XC models)</li> <li>nShield Remote Administration (purchased separately)</li> <li>nShield Monitor (purchased separately)</li> <li>Secure audit logging</li> <li>Syslog diagnostics support and Windows performance monitoring</li> <li>SNMP monitoring agent</li> </ul>	<ul style="list-style-type: none"> <li>Standard 1U 19in. rack mount Dimensions: 43.4 x 430 x 705mm (1.7 x 16.9 x 27.8in)</li> <li>Weight: 11.5kg (25.4lb)</li> <li>Input voltage: 100-240V AC auto switching 50-60Hz</li> <li>Power consumption: up to 2.0A at 110V AC, 60Hz   1.0A at 220V AC, 50Hz</li> <li>Heat dissipation: 327.6 to 362.0 BTU/hr (full load)</li> <li>Reliability - MTBF (hours)<sup>3</sup>, Connect XC: 107,384 hours, Connect+: 99,284 hours</li> </ul>

Note 3: Calculated at 25 degrees centigrade operating temperature using Telcordia SR-332 "Reliability Prediction Procedure for Electronic Equipment" MTBF Standard

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/HSM](https://entrust.com/HSM)



Contact us:  
[HSMinfo@entrust.com](mailto:HSMinfo@entrust.com)