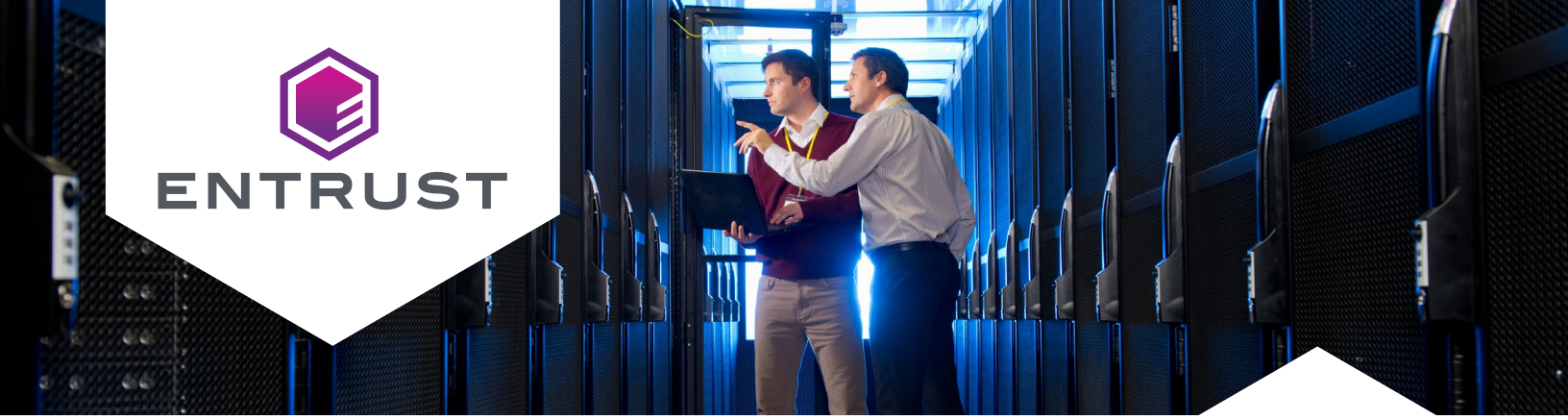

Entrust nShield Post-Quantum Option Pack

The Entrust nShield Post-Quantum Option Pack enables post-quantum cryptographic applications for nShield HSMs.

HIGHLIGHTS

- Protect sensitive applications and documents using NIST's quantum-resistant algorithms within the FIPS-certified boundary of nShield HSMs
- Evolve your organization with emerging post-quantum (PQ) standards and align crypto security requirements with organizational PQ strategy
- Integrate with Entrust's composite digital certificates to create quantum-resistant, long-life digital certificates

Prepare for post-quantum cryptography (PQC) with the Post-Quantum Option Pack and nShield HSMs

The Entrust nShield Post-Quantum Option Pack leverages the Entrust CodeSafe SDK and the liboqs open source library to make quantum-resistant cryptographic algorithms available to customers.

It supports NIST's PQC algorithms identified for standardization including CRYSTALS-Dilithium, FALCON, and SPHINCS+ digital signature algorithms, and the CRYSTALS-Kyber key encapsulation mechanism, inside the FIPS 140-2/140-3 Level 3 physical boundary of an nShield HSM. Customers with an nShield FIPS Level 3 HSM and the nShield Post-Quantum Option Pack can generate quantum-resistant keys inside the HSM, protected by FIPS 140-2 Level 3 Security World standard mechanisms, and carry out key signing, digital signature, encryption, decryption, and key exchange.

nShield Post-Quantum Option Pack and CodeSafe combine for many applications

The nShield Post-Quantum Option Pack, in conjunction with CodeSafe, can be used to protect any type of application. Examples include cryptography and high-value business logic associated with banking, smart metering, authentication agents, digital signature agents, and custom encryption processes.

About CodeSafe

CodeSafe is a software development kit that enables developers to write and execute sensitive applications in the tamper-resistant boundary of an nShield HSM. Applications running in the secure environment can encrypt, decrypt, and process data as well as benefit from HSM enforcement of policies that govern use of the applications' keys.

Entrust nShield Post-Quantum Option Pack

Ensure PQC application integrity

The nShield Post-Quantum Option Pack provides tools to digitally sign the applications running in nShield's secure execution environment so their integrity can be verified by the HSM at runtime.

KEY FEATURES & BENEFITS

Implement PQC in a secure HSM

The nShield Post-Quantum Option Pack integrates the quantum-resistant digital signature and key exchange algorithms selected by NIST for its PQC standard, so you can test the use of the algorithms with your applications in a representative, secure environment — not just an emulation or software library.

Get future-ready experience

Gain experience with the unique requirements and characteristics of quantum-resistant cryptography, including longer key lengths.

Adopting this solution will allow you to align cryptographic security requirements with organizational post-quantum strategy.

Create composite certificates

With the nShield Post-Quantum Option Pack applications can generate composite signatures to create PQ-resistant long-life digital signatures and certificates. Composite signatures combine classical cryptographic algorithms and post-quantum algorithms for added resilience and assurance.

nShield compatibility

The nShield Post-Quantum Option Pack is compatible with FIPS Level 3 HSMs from the nShield XC and nShield 5 product line.

Getting started with the nShield Post-Quantum Option Pack

To use the nShield Post-Quantum Option Pack, you will need:

- FIPS Level 3 nShield HSM
- CodeSafe developer toolkit
- CodeSafe activation license

The CodeSafe developer toolkit includes tutorials, documentation, and sample programs to help you integrate your application with nShield HSMs. The Entrust Professional Services team is also available to assist you with your integration.

HSM development environment

CodeSafe is compatible with the following programming environments:

- C and C++ programming languages for embedded applications
- C, C++, and Java on host server

Entrust nShield Post-Quantum Option Pack

SUPPORTED POST-QUANTUM CRYPTOGRAPHY ALGORITHMS

(Subset of liboqs Open Quantum Safe (OQS) library):

FALCON
- FALCON-512
- FALCON-1204

CRYSTALS-Dilithium
- Dilithium2
- Dilithium3
- Dilithium3-AES
- Dilithium5
- Dilithium5-AES

Rainbow
- Rainbow-I-Classic
- Rainbow-I-Circumzenithal
- Rainbow-I-Compressed
- Rainbow-III-Classic
- Rainbow-III-Circumzenithal
- Rainbow-III-Compressed
- Rainbow-V-Classic
- Rainbow-V-Circumzenithal
- Rainbow-V-Compressed

Picnic
- Picnic-L1-FS
- Picnic-L1-UR
- Picnic-L1-full
- Picnic-L3-FS
- Picnic-L3-UR
- Picnic-L3-full
- Picnic-L5-FS
- Picnic-L5-UR
- Picnic-L5-full
- Picnic3-L1
- Picnic3-L3
- Picnic3-L5

SPHINCS+-SHA256
- SPHINCS+-SHA256-128f-robust
- SPHINCS+-SHA256-128f-simple
- SPHINCS+-SHA256-128s-robust
- SPHINCS+-SHA256-128s-simple
- SPHINCS+-SHA256-192f-robust
- SPHINCS+-SHA256-192f-simple
- SPHINCS+-SHA256-192s-robust
- SPHINCS+-SHA256-192s-simple
- SPHINCS+-SHA256-256f-robust
- SPHINCS+-SHA256-256f-simple
- SPHINCS+-SHA256-256s-robust
- SPHINCS+-SHA256-256s-simple

SPHINCS+-Haraka
- SPHINCS+-Haraka-128f-robust
- SPHINCS+-Haraka-128f-simple
- SPHINCS+-Haraka-128s-robust
- SPHINCS+-Haraka-128s-simple
- SPHINCS+-Haraka-192f-robust
- SPHINCS+-Haraka-192f-simple
- SPHINCS+-Haraka-192s-robust
- SPHINCS+-Haraka-192s-simple
- SPHINCS+-Haraka-256f-robust
- SPHINCS+-Haraka-256f-simple
- SPHINCS+-Haraka-256s-robust
- SPHINCS+-Haraka-256s-simple

SPHINCS+-SHAKE256
- SPHINCS+-SHAKE256-128f-robust
- SPHINCS+-SHAKE256-128f-simple
- SPHINCS+-SHAKE256-128s-robust
- SPHINCS+-SHAKE256-128s-simple
- SPHINCS+-SHAKE256-192f-robust
- SPHINCS+-SHAKE256-192f-simple
- SPHINCS+-SHAKE256-192s-robust
- SPHINCS+-SHAKE256-192s-simple
- SPHINCS+-SHAKE256-256f-robust
- SPHINCS+-SHAKE256-256f-simple
- SPHINCS+-SHAKE256-256s-robust
- SPHINCS+-SHAKE256-256s-simple

CRYSTALS-Kyber
- Kyber512
- Kyber512-90s
- Kyber768
- Kyber768-90s
- Kyber1024
- Kyber1024-90s

Learn more

Learn more about the nShield Post-Quantum Option Pack and nShield HSMs at **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications, and data, visit **entrust.com**.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223