Entrust nShield Post-Quantum Software Development Kit (SDK)

The Entrust nShield Post-Quantum SDK enables post-quantum cryptographic applications for nShield HSMs with the CodeSafe SDK.

HIGHLIGHTS

- Protect sensitive applications and documents, use NIST's quantum-resistant algorithms within the FIPS-certified boundary of nShield HSMs
- Evolve your organization with emerging PQ standards and align crypto security requirements with organizational post-quantum 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 SDK, nShield HSMs, and CodeSafe

Entrust has developed a representative test environment for PQ algorithms that leverages the Entrust CodeSafe SDK and the liboqs open source library to make available quantum-resistant cryptographic algorithms.

The Entrust nShield Post Quantum SDK supports NIST's PQC algorithms identified for standardization including CRYSTALS-Dilithium, FALCON, and SPHINCS+ digital signature algorithms, inside the FIPS 140-2 Level 3 physical boundary of an nShield HSM.

Customers with an nShield FIPS Level 3 HSM, CodeSafe, and the nShield Post-Quantum SDK can generate quantum-resistant keys inside the HSM and carry out key signing, digital signature, encryption, decryption, and key exchange.

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.

nShield Post-Quantum SDK and CodeSafe combine for many applications

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

Learn more at entrust.com/HSM

Entrust nShield Post-Quantum SDK

Ensure PQC application integrity

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

KEY FEATURES & BENEFITS

Test and implement post-quantum cryptography in a secure HSM

The nShield Post-Quantum SDK integrates the quantum-resistant digital signature algorithms selected by NIST for its post-quantum cryptographic 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

The nShield Post-Quantum SDK supports the creation of Entrust composite digital certificates to create PQ-resistant long-life digital certificates. Composite digital certificates combine classical cryptographic algorithms and post-quantum algorithms for added resilience and assurance.

nShield compatibility

The nShield PQ SDK and the CodeSafe SDK are available with FIPS 140-2 Level 3 certified nShield Solo PCIe HSMs and network-attached nShield Connect HSMs, including the XC product line.

Getting started with the nShield Post-Quantum SDK

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

- FIPS 140-2 Level 3 certified nShield Solo or Connect HSM
- nShield Post-Quantum SDK
- 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 SDK

SUPPORTED POST-QUANTUM CRYPTOGRAPHY ALGORITHMS

(Subset of Lib 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

Learn more

Learn more about the nShield Post-Quantum SDK 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