Entrust CodeSafe 5®

Certified hardware protection for sensitive applications

HIGHLIGHTS

CodeSafe 5: Execute code in a secure environment while addressing Zero Trust initiatives

- Protects sensitive applications by executing them inside tamper-resistant hardware security modules (HSMs)
- Helps ensure integrity by digitally signing and verifying code
- Provides a secure environment for key management and custom algorithms through policy enforcement
- Delivers strong access control by uniquely associating keys and certificates to applications
- CodeSafe 5 applications can be remotely managed using Entrust KeySafe 5

CodeSafe 5 is a protected environment that enables developers to write and execute sensitive applications inside the tamper-resistant boundary of FIPS-certified nShield HSMs. Applications running in the secure execution environment can encrypt, decrypt, and process data as well as benefit from HSM enforcement of the policies that govern use of the applications' keys.

Wide range of applications

CodeSafe 5 can be used to protect any type of application, and can be used as part of an organization's Zero Trust journey. Examples include cryptography and high-value business logic associated with banking, smart metering, authentication agents, digital signature agents, post-quantum investigative projects, and blockchain/digital wallets.

Ensuring CodeSafe 5 application integrity

CodeSafe 5 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.

Learn more about CodeSafe 5 at entrust.com

Entrust CodeSafe 5®

KEY FEATURES & BENEFITS

CodeSafe key policy enforcement and access control

CodeSafe allows the software owner to define the policies governing the usage of application data — including keys and certificates — and enforces these policies, providing a secure environment for key management. CodeSafe also uniquely associates the keys and certificates to designated applications to ensure strong access control.

Remote deployment and updates

Administrators can deploy applications from a central location, avoiding the need to physically access HSMs.

nShield compatibility

CodeSafe 5 is available with FIPS 140-3 Level 3 certified* nShield PCIe and network-attached nShield HSMs.

nShield Post-Quantum SDK

The Entrust nShield Post-Quantum SDK enables post-quantum cryptographic applications for nShield HSMs leveraging CodeSafe. It supports NIST's PQC algorithms identified for standardization including CRYSTALS-Dilithium, FALCON, and SPHINCS+ digital signature algorithms. Separate data sheet with further details available on request.

HSM development environment

CodeSafe 5 is based on a protected Linux container environment with standard host API.

CodeSafe 5 programming environments:

- C and C++
- Python
- C, C++, and Java on the host environment

*The FIPS 140-3 Level 3 certification status is currently in review.

Learn more about CodeSafe 5 at entrust.com

Entrust CodeSafe 5®

Getting started with CodeSafe 5

To use CodeSafe 5, you will need:

- FIPS 140-3 Level 3 nShield HSM
- CodeSafe 5 developer toolkit
- CodeSafe 5 activation license

The CodeSafe 5 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.

Learn more

A CodeSafe white paper is available on request providing a more in-depth discusssion on the underlying technology. To find out more about Entrust nShield HSMs visit **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