Entrust CodeSafe®

Certified hardware protection for sensitive applications

HIGHLIGHTS

CodeSafe: execute code in a secure environment

- 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 through policy enforcement
- Delivers strong access control by uniquely associating keys and certificates to applications
- Offers a convenient solution using remote CodeSafe tools

CodeSafe is a set of tools that enable 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 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.

Ensuring CodeSafe application integrity

CodeSafe 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.

Entrust CodeSafe®

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.

Secure SSL/TLS endpoints

CodeSafe application developers can embed the OpenSSL library within their application to terminate SSL/TLS sessions inside the nShield HSM, facilitating end-to-end encryption and strengthening the security of the data transport layer and reducing the attack surface.

Remote deployment and updates

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

nShield compatability

CodeSafe is available with FIPS 140-2 Level 3 certified nShield Solo PCIe and network-attached nShield Connect HSMs. Compatible models include all supported nShield Solo and Connect HSMs including the XC product line.

HSM development environment

CodeSafe is compatible with the following programming applications:

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

Getting started with CodeSafe

To use CodeSafe, you will need:

- FIPS 140-2 Level 3 certified nShield Solo or Connect 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.

Learn more

A CodeSafe whitepaper 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/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com