



ENTRUST



CodeSafe® de Entrust

Protección certificada de hardware para aplicaciones sensibles

CARACTERÍSTICAS GENERALES

CodeSafe: ejecuta el código en un entorno seguro

- Protege las aplicaciones confidenciales ejecutándolas dentro de módulos de seguridad de hardware (HSM), que son a prueba de manipulaciones indebidas
- Ayuda a garantizar la integridad firmando y verificando el código de forma digital
- Proporciona un entorno seguro para la administración de claves a través de la aplicación de políticas
- Ofrece un fuerte control de acceso al asociar exclusivamente las claves y los certificados a las aplicaciones
- Ofrece una solución cómoda utilizando herramientas remotas CodeSafe

CodeSafe es un conjunto de herramientas que permite a los desarrolladores escribir y ejecutar aplicaciones sensibles dentro del límite resistente a las falsificaciones de HSM nShield con certificación FIPS. Las aplicaciones que funcionan en un entorno de ejecución seguro pueden cifrar, descifrar y procesar datos, así como beneficiarse de la aplicación HSM de las políticas que administran el uso de las claves de las aplicaciones.

Amplio rango de aplicaciones

CodeSafe puede utilizarse para proteger cualquier tipo de aplicaciones. Ejemplos incluyen criptografía y lógica empresarial de alto valor asociada a la banca, medición inteligente, agentes de autenticación, agentes de firma digital y procesos de encriptación personalizados.

Garantizar la integridad de la aplicación CodeSafe

CodeSafe proporciona herramientas para firmar digitalmente las aplicaciones que se ejecutan en el entorno de ejecución segura de nShield para que el HSM pueda verificar su integridad en el tiempo de ejecución.



CodeSafe® de Entrust

PRESTACIONES Y BENEFICIOS PARA CLAVES

Control de acceso y aplicación de políticas de claves de CodeSafe

CodeSafe permite al propietario del software definir las políticas que gestionan el uso de datos de la aplicación, incluyendo claves y certificados, y aplica estas políticas, proporcionando un entorno seguro para la gestión de claves. CodeSafe también asocia exclusivamente las claves y los certificados para las aplicaciones designadas a fin de garantizar un control de acceso sólido.

Crterios de valoración SSL/TLS seguros

Los desarrolladores de la aplicación CodeSafe pueden integrar la biblioteca OpenSSL dentro de su aplicación para finalizar las sesiones SSL/TLS dentro del HSM nShield, facilitando la encriptación integral y fortaleciendo la seguridad del nivel de transporte de datos y reduciendo la superficie de ataque.

Implementación y actualizaciones remotas

Los administradores pueden implementar aplicaciones desde una ubicación central, evitando la necesidad para acceder físicamente a los HSM.

Compatibilidad nShield

CodeSafe está disponible con los HSM nShield Solo y nShield Connect con certificación FIPS 140-2 de nivel 3. Los modelos compatibles incluyen todos los HSMs nShield Solo y Connect compatibles, incluida la línea de productos XC.

Entorno de desarrollo de HSM

CodeSafe es compatible con las siguientes aplicaciones de programación:

- Lenguajes de programación C y C++ para aplicaciones integradas
- C, C++ y Java en el servidor

Empezar con CodeSafe

Para utilizar CodeSafe, necesitará:

- HSM nShield Solo o Connect con certificación FIPS 140-2 de nivel 3
- Conjunto de herramientas de desarrollador CodeSafe
- Licencia de activación CodeSafe

El conjunto de herramientas de CodeSafe para desarrollador incluye tutoriales, documentación y programas de muestra para ayudarle a integrar su aplicación con los HSM nShield. El equipo de Servicios profesionales de Entrust también está disponible para ayudarle con su integración.

Más información

Hay documentación de CodeSafe disponible bajo petición proporcionando información más detallada sobre la tecnología subyacente. Para saber más sobre los HSM nShield de Entrust visite entrust.com/HSM. Para saber más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite entrust.com



Más información

entrust.com/HSM



ENTRUST