Entrust CodeSafe®

중요한 애플리케이션을 위한 인증받은 하드웨어 보호

하이라이트

CodeSafe: 안전한 환경에서 코드를 실행합니다

- 중요한 애플리케이션을 변조 방지 하드웨어 보안 모듈(HSM) 내에서 실행해서 보호합니다
- 디지털 서명과 인증 코드로 무결성을 보장합니다
- 정책 집행을 통해 키 관리를 위한 안전한 환경을 제공합니다
- 키와 인증서를 애플리케이션에 고유하게 연결하여 강력한 접근 제어를 제공합니다
- 원격 CodeSafe 도구를 사용하여 편리한 솔루션을 제공합니다

CodeSafe는 개발자가 FIPS 인증 nShield HSM의 변조 방지 경계 내에서 중요한 애플리케이션을 작성 및 실행할 수 있도록 돕는 도구 모음입니다. 안전한 실행 환경 내에서 실행되는 애플리케이션은 데이터를 암호화, 암호 해독 및 처리함에 더불어 애플리케이션 키의 사용을 통제하는 정책의 HSM 집행의 혜택도 누릴 수 있습니다.

광범위한 애플리케이션

CodeSafe는 모든 종류의 애플리케이션을 보호하는 데 사용할 수 있습니다. 예를 들어 암호화, 은행에 관련된 고가치 비즈니스 로직, 스마트 미터링, 인증 에이전트, 디지털 서명 에이전트 및 커스텀 암호화 프로세스 등이 포함됩니다.

CodeSafe 애플리케이션 무결성 보장

CodeSafe는 nShield의 안전한 실행 환경 내 실행되는 애플리케이션에 디지털 서명을 하여 런타임 내 HSM에 의해 무결성을 검증 받도록 하는 도구를 제공합니다.

Entrust CodeSafe®

주요 기능 및 혜택

CodeSafe 키 정책 집행 및 접근 제어

CodeSafe는 소프트웨어 소유자가 키와 인증서를 포함한 애플리케이션 데이터의 사용을 관리하는 정책을 정의하고 이러한 정책을 시행하여 키 관리를 위한 안전한 환경을 제공할 수 있도록 합니다. 또한 CodeSafe는 강력한 접근 제어를 보장하기 위해 지정된 애플리케이션에 키와 인증서를 고유하게 연결합니다.

안전한 SSL/TLS 엔드포인트

CodeSafe 애플리케이션 개발자는 nShield HSM 내에서 SSL/TLS 세션을 종료하기 위해 애플리케이션 내 OpenSSL 라이브러리를 내장하여, 엔드투엔드 암호화를 촉진하고 데이터 전송 계층의 보안을 강화하며 공격 표면을 줄일 수 있습니다.

원격 배포 및 업데이트

관리자는 HSM에 물리적으로 접근할 필요 없이 중앙에서부터 애플리케이션을 배포할 수 있습니다.

nShield 호환성

CodeSafe는 FIPS 140-2 레벨 3 인증 nShield 솔로 PCIe 및 네트워크에 연결된 nShield 커넥트 HSM과 함께 제공됩니다. 호환되는 모듈로는 XC 제품군을 포함하여 지원되는 모든 nShield 솔로 및 커넥트 HSM이 있습니다.

HSM 개발 환경

CodeSafe는 다음과 같은 프로그래밍 애플리케이션과 호환됩니다.

- 임베디드 애플리케이션의 C 및 C++ 프로그래밍 언어
- 호스트 서버의 C, C++ 및 Java

CodeSafe 시작하기

CodeSafe를 사용하려면 다음이 필요합니다.

- FIPS 140-2 레벨 3 인증을 받은 nShield 솔로 또는 커넥트 HSM
- CodeSafe 개발자 툴킷
- CodeSafe 활성화 라이선스

CodeSafe 개발자 툴킷에는 nShield HSM과 애플리케이션의 통합을 돕기 위한 튜토리얼, 문서 및 샘플 프로그램이 포함됩니다. Entrust 전문 서비스 팀 또한 통합을 도와드릴 수 있습니다.

자세히 보기

요청하시면 받아보실 수 있는 CodeSafe 백서는 기반 기술에 대한 보다 심도 있는 논의를 다룹니다. Entrust nShield HSM에 대해 더 알아보시려면 **entrust.com/HSM**을 방문하십시오. 신원, 접근, 소통 및 데이터에 관련된 Entrust의 디지털 보안 솔루션에 대해 더 알아보시려면 **entrust.com**을 방문하십시오.

에서 자세히 보기
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com