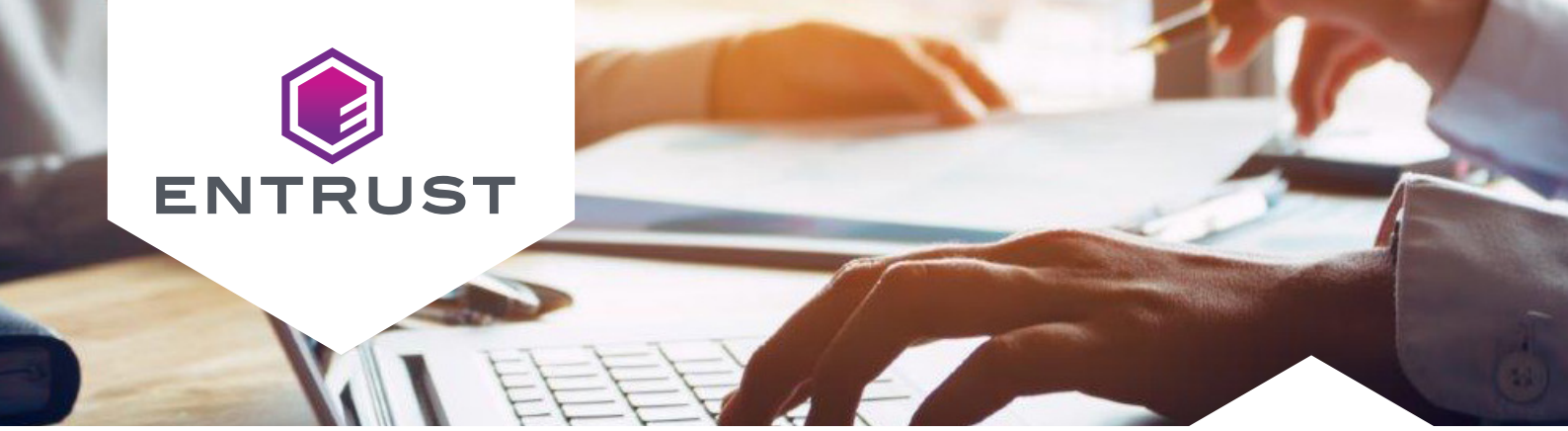

Entrust 코드 서명 솔루션

코드 서명을 위한 고보장성 보안

하이라이트

- 저자, 출판 날짜, 내용 보호
- 소프트웨어 무결성 구축
- 귀중한 코드 서명 키 보호

코드 배포 문제

비즈니스 IT는 복잡한 부문으로, 다양한 소스의 소프트웨어를 사용하여 조직을 운영합니다. 사내용이든 고객에게 판매하는 용도이든 소프트웨어를 개발하는 기업은 소프트웨어의 진위를 증명하는 메커니즘을 만들거나 지원해야 합니다. 이 보안을 보장하려면 다음과 같은 기능이 필요합니다.

- 서명 절차를 검증하여 올바른 키로 올바른 코드만 서명하는 기능
- 개인 서명 키를 관리하여 무단 제품이 고객에게 전해지지 않도록 도난 방지
- 모든 서명 활동에 대한 감사 기록 제공

Entrust는 절차와 무결성, 권한 부여, 개인 키 보호 문제를 해결하는 보안 코드 서명 솔루션의 개발과 구현에 관련된 상당한 전문 지식을 보유하고 있으며 다음 성능을 제공합니다.

- 키 도난, 기업 사칭 사기, 악성 소프트웨어 개조 위험 감소
- 최종 사용자가 소프트웨어의 소스와 무결성을 확인하고 악성 코드 변경이나 삽입을 감지하도록 지원
- 서명되지 않은 소프트웨어에 대한 운영 체제의 강력한 경고 메시지로 인해 사용자가 설치를 중단하는 것을 방지
- 코드 서명 작업에 대한 액세스 제어, 승인 워크플로, 자동화, 감사 기능 제공

이러한 기능을 제공하기 위해 Entrust는 신뢰점 역할을 담당하는 nShield® 하드웨어 보안 모듈(HSM)을 기반으로 두 가지 코드 서명 솔루션을 제공합니다. 솔루션은 다음과 같습니다.

- Code Signing Gateway
- 직접적인 HSM 통합을 통한 코드 서명

코드란?

코드는 대상 플랫폼에서 사용하거나 실행하는 정보의 바이너리 패키지라고 할 수 있습니다. 코드의 예로는 실행 패키지, 설치 프로그램 패키지, 펌웨어 패키지, 임베디드 환경이 있습니다.

ENTRUST.COM/HSM에서 자세히 보기

Entrust 코드 서명 솔루션

Entrust HSM을 신뢰점으로 사용하는 코드 서명

코드 서명은 소프트웨어 출판에 디지털 서명을 적용하는 것입니다. 코드 서명을 통해 최종 사용자는 게시자의 신원을 인증하여 소프트웨어의 출처와 무결성을 확인할 수 있습니다. 또한 서명되지 않은 소프트웨어에 대한 운영 체제의 강력한 경고 메시지로 인해 사용자가 소프트웨어 설치를 포기하는 것을 방지합니다.

코드 서명 솔루션은 소프트웨어 제작업체의 공개/개인 키 페어에 더불어 소프트웨어 제작업체의 공개 키를 포함하고 적합한 CA에서 서명한 디지털 인증서를 사용하여, 최종 사용자가 코드를 검증할 수 있도록 합니다. 소프트웨어 제작업체가 배포할 코드를 해시화하고, 개인 키를 사용하여 해시 서명/암호화를 완료하는 것으로 절차가 시작됩니다. 그런 다음 암호화된 해시와 원본 코드를 디지털 인증서와 함께 패키지로 최종 사용자에게 배포합니다. 마지막 단계로 최종 사용자는 소프트웨어 제작업체의 공개 키를 사용하여 암호화된 해시 코드를 복호화하고 결과로 나타나는 해시를 수신된 코드의 재생성된 해시와 비교합니다. 해시가 동일하면 코드가 확인됩니다.

개인 키는 코드 서명 시스템의 보안에 핵심적이며 절대 공개하거나 공유해서는 안 됩니다. 개인 키가 손상되면 보안 시스템에 장애가 일어납니다. 개인 서명 키 보안은 코드 서명 절차의 기반입니다.

코드 서명과 같이 민감한 애플리케이션의 경우, 사용 여부와 상관없이 개인 키를 보호하는 것은 안전한 솔루션을 만드는 데 있어 매우 중요합니다. HSM은 인증받은 변조 방지 환경을 제공하여 수명 주기 동안 키를 보호합니다.

Code Signing Gateway

고도의 제어 수준을 갖춘 소프트웨어 서명 승인 절차가 필요한 대규모 조직을 위해 Code Signing Gateway는 소프트웨어 개발 기업에 유연한 중앙 집중식 워크플로 자동화 기능을 광범위하게 제공하여, 강력한 보안 요건을 충족할 수 있도록 지원합니다. Code Signing Gateway는 Entrust 코드 서명 워크플로 애플리케이션을 실행하는 중앙 집중식 고객 호스팅 서버입니다.

Code Signing Gateway는 워크플로 관리, 요청 수락, 승인자 이메일 통지, 시간제한 관리, 승인 확인, 활동 기록, 서명된 코드를 대기 구역에 전달하는 기능을 담당합니다. 예를 들어 Code Signing Gateway 관리자, 기업, 데스크톱, IoT 또는 모바일 애플리케이션 개발자, 관리부서, 코드 서명 승인자를 비롯한 여러 사용자 역할을 지원할 수 있습니다. Active Directory 통합은 작업 그룹 권한 부여와 사용자 인증에 사용됩니다.

nShield 범용 HSM

nShield HSM은 다양한 애플리케이션에 사용되는 키를 생성하고 보호하기 위해 안전한 환경을 제공하며, 인증받고 강화된 변조 방지 장치입니다. 서비스로서의 nShield HSM은 세 가지 폼 팩터로 제공됩니다.

- nShield Connect, 네트워크를 통해 여러 애플리케이션을 제공하는 장치이며 서비스 형태로도 사용 가능
- nShield Solo, 단일 서버에서 애플리케이션을 지원하는 PCIe 카드
- nShield Edge, 저용량 처리용 USB 연결 데스크톱 장치

nShield HSM은 FIPS 140-2 레벨 2, 레벨 3 인증을 받았습니다.

ENTRUST.COM/HSM에서 자세히 보기

Entrust 코드 서명 솔루션

nShield HSM은 코드 서명에 사용되는 개인 키를 보호하는 데 사용됩니다. 서명 키는 HSM에 보관되며 Code Signing Gateway에서 생성할 수 있는 여러 서명 프로필에 매핑됩니다.

Code Signing Gateway는 Oracle Jarsigner, Microsoft SignTool, Apple 코드 서명 도구, Android 코드 서명 유틸리티와 같은 표준 서명 도구와 통합 가능합니다. 절차를 나타내는 도표는 그림 1과 같습니다.

추가 기능에는 다중 서명 프로필을 포함하여 다중 서명 프로필, 중앙 집중식 로깅, 파일 보관, 타임 스탬프 서비스와의 통합을 지원하고 여러 디지털 인증서를 활용하도록 정의합니다. 또한, 서명 전에 파일에서 바이러스를 검사하기 위한 Microsoft Defender와의 통합을 포함합니다.

Entrust Code Signing Gateway는 Entrust 전문 서비스팀을 통해 고객사의 고유한 환경에 따라 제공하는 맞춤형 솔루션입니다.

직접적인 HSM 통합을 통한 코드 서명

nShield HSM과의 직접 통합은 간단한 역할 분리로 소수의 개발자에게 솔루션을 제공합니다. 일반적으로 개별 개발자 워크스테이션이나 전용 코드 서명 서버를 대상으로 사용됩니다. 코드 서명에 사용되는 개인 키는 nShield HSM이 생성하고 보호합니다.

코드 서명은 JCE(Java Cryptography Extension), Microsoft CAPI, CNG와 같은 표준 API를 사용하여 HSM과 통합되며 Jarsigner, SignTool, Open SSL과 같은 타사 도구를 사용하여 HSM 실행용 서명 요청을 생성합니다.

관련 링크

entrust.com/HSM을 방문하면 Entrust nShield HSM에 관해 자세히 알아보실 수 있습니다. **entrust.com**을 방문하면 Entrust의 신원, 접근, 통신, 데이터 관련 디지털 보안 솔루션에 관해 자세히 알아보실 수 있습니다.

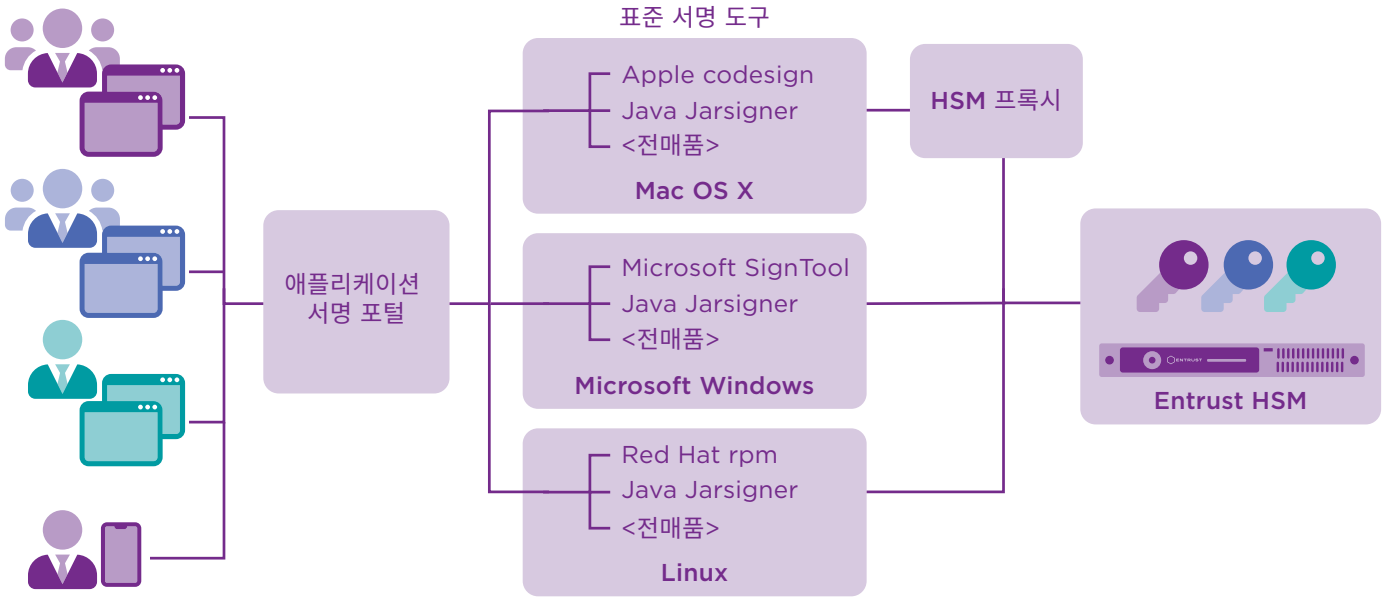

그림 1. Code Signing Gateway 도표

Entrust nShield HSM
관련 정보 확인 및 문의

HSMinfo@entrust.com

entrust.com/HSM

ENTRUST CORPORATION 소개

Entrust는 믿을 수 있는 신원, 결제 및 데이터 보호를 가능케 함으로써 안전한 세상을 유지합니다. 사람들은 국경을 넘고, 구매를 하고, 전자 정부 서비스에 접속하고 기업 네트워크에 로그인하는 것이 원활하고 안전한 경험이기를 오늘날, 그 어느 때보다도 더 요구합니다. Entrust는 이와 같은 모든 상호작용의 핵심에 있는 디지털 보안 및 자격 증명 발급 솔루션에 있어 견줄 데 없는 다양성을 자랑합니다. 2,500명도 넘는 동료, 글로벌 파트너로 구성된 네트워크, 그리고 150개국 이상의 고객을 보유한 당사는 세계에서 가장 신뢰 받는 기관들의 신뢰를 받고 있습니다.

에서 자세히 보기:
entrust.com/HSM

ENTRUST

연락처:
HSMinfo@entrust.com