강화된 보안: Red Hat 인증 시스템을 위한 Entrust의 고보장성 키 보호

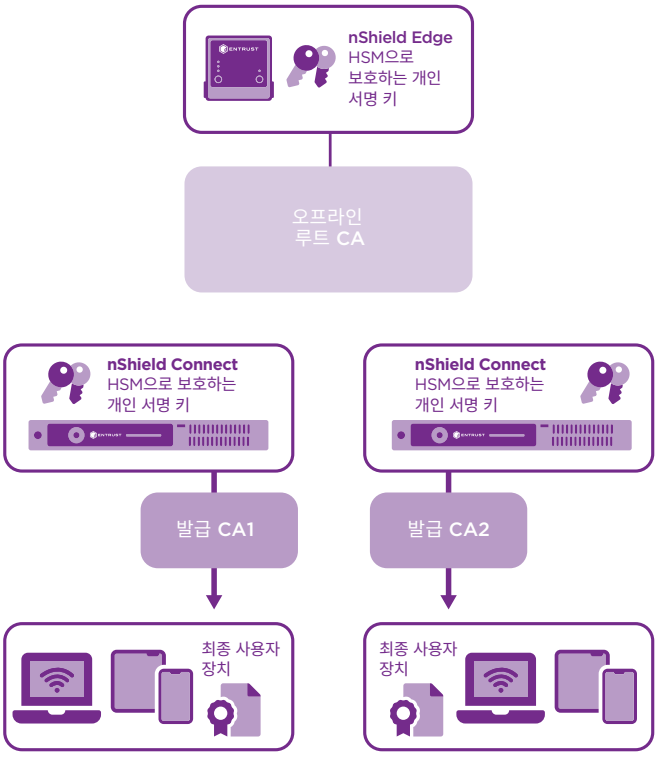
공개 키 기반 구조(PKI)에 대한 신뢰 구축

하이라이트

- NSA CSfC(Commercial Solutions for Classified) 애플리케이션을 위한 Red Hat 인증 시스템의 보안 확장
- 사용자 신원을 관리하고 통신을 비공개로 유지하는 보안 프레임워크 강화
- 트랜잭션과 PKI 지원 애플리케이션 보호
- NIST FIPS 140-2 인증 Entrust nShield® 하드웨어 보안 모듈(HSM) 사용

문제점: 비즈니스 애플리케이션 증가에 대응하는 과정에서 기업 PKI의 부담 확대

데이터 침해 기술이 더욱 정교해지면서 조직은 중요한 애플리케이션과 민감한 데이터에 대한 액세스를 보호하고 제어하기 위해 PKI로 전환했습니다. PKI 내에서 인증 기관(CA)은 온라인 ID를 확인하고 액세스 제어를 시행하기 위해 전자 자격 증명을 발급합니다. 사용되는 디지털 인증서의 수, 지원하는 애플리케이션의 중요성과 가치, 애플리케이션이 정부나 산업 규제 준수에 따른 고난도 감시 대상인지를 분석하는 것은 PKI가 증가하는 수요를 충족하도록 하는 중요한 요소입니다.



nShield HSM은 Red Hat 인증 시스템에서 사용하는 개인 키를 보호합니다.

ENTRUST.COM/HSM에서 자세히 보기

Red Hat 인증 시스템을 위한 고보장성 키 보호

과제: 신원 및 액세스 제어를 위한 신뢰점 구축

PKI를 뒷받침하는 CA의 무결성과 보안을 보호하는 것은 비즈니스 애플리케이션과, 비즈니스 애플리케이션이 보호하는 데이터에 대한 신뢰를 보장하는 데 매우 중요합니다. PKI가 모바일 및 BYOD(Bring Your Own Device)를 포함하여 변화하는 사용자 액세스 토폴로지를 점점 더 많이 지원함에 따라 조직은 개인 암호키를 신뢰할 수 있는 방식으로 보호하고 관리해야 합니다.

솔루션: Red Hat과 Entrust가 함께 제공하는 강력한 디지털 신원 보호

Red Hat 인증 시스템은 개인, 장치 또는 서비스를 해당 개인 키에 바인딩하는 데 사용되는 디지털 ID를 발급, 관리, 검증합니다. 발급된 각 인증서의 유효성은 ID를 발급하는 CA 키를 보호하는 데 달려있습니다. 로컬 파일로 보관한 키를 사용하여 서버에서 발급 절차를 실행하면 해당 키가 복제, 수정, 치환에 취약해질 수 있습니다. 오늘날 대부분의 CA는 조직 내에서 사용할 인증서를 발급하는 데 사용됩니다. 인증서는 보통 내부적으로 유무선 인증, SSL/TLS(보안 소켓 계층/전송 계층 보안) 연결, VPN(가상 사설망) 인증 실행에 사용됩니다. 애플리케이션을 확장하려면 PKI 서비스가 필요하기 때문에 CA에 대한 요구와 보안 강화에 대한 요구가 무엇보다 중요합니다.

Entrust nShield HSM은 개인 루트를 보호하고 CA 키에 서명하여 PKI의 보증 수준을 높입니다. 또한, 발급, 관리, 검증 절차를 보호하여 조직이 신원과 액세스 솔루션을 강화할 수 있도록 합니다. 이에 더해 CAPI(표준 암호화 애플리케이션 프로그래밍 인터페이스)를 사용하여 Red Hat 인증 시스템과 쉽게 통합됩니다. Entrust nShield HSM을 사용하면 모든 인증서 발급과 유효성 검사가 HSM의 보호 범위 내에서 처리됩니다. 개인 루트와 서명 키는 HSM 외부 액세스가 불가능하며 외부에서 읽을 수 없는 형식으로 되어 있습니다. nShield HSM은 백업, 보관, 복구 과정에서도 개인 키가 조작되거나 훼손되지 않도록 보장합니다.

Red Hat 인증 시스템을 위한 고보장성 키 보호

Red Hat 인증 시스템과 함께 Entrust HSM을 사용해야 하는 이유

침해 식별, 복구, 비상 계획은 PKI의 보안을 강화하기 위해 실행할 수 있는 중요한 절차입니다. 강화된 고보장성 PKI는 보안에 중요한 키를 도난과 오용으로부터 보호하는 환경을 제공합니다. Entrust nShield HSM을 사용하여 인증서 발급을 신원 확인과 승인에 바인딩하는 것은 과거의 CA 보안 침해 사례를 통해 얻은 중요한 가르침입니다.

FIPS 140-2 레벨 3과 CC 인증 EAL4+ 포함, 엄격한 보안 표준 인증을 받은 nShield HSM의 성능은 다음과 같습니다.

- 보안 및 변조 방지 환경에서 디지털 인증서 서명과 발급을 위한 키 보관
- 스마트카드 기반 정책과 2단계 인증으로 관리자 액세스 관리
- 공공 부문, 금융 서비스, 기업 관련 규제 요건 준수

Entrust HSM

Entrust nShield HSM은 현재 이용 가능한 솔루션 중에서도 최고 성능을 갖추었으며 가장 안전하고 통합하기 쉬운 HSM 솔루션 중 하나로, 규정 준수를 촉진하고 기업, 금융 기관과 정부 기관에 최고 수준의 데이터 보안과 애플리케이션 보안을 제공합니다. Entrust만의 Security World 키 관리 아키텍처를 이용하면 강력하고 세분화된 방식으로 키 액세스와 사용을 통제할 수 있습니다.

RED HAT

Red Hat은 엔터프라이즈 오픈소스 솔루션을 제공하는 세계적인 기업입니다. Red Hat Certificate System 외에도 다양한 관리 및 서비스 중에서 Red Hat Enterprise Linux, Red Hat OpenStack, 및 Red Hat OpenShift 플랫폼이 솔루션에 포함됩니다. Entrust nShield HSM은 Red Hat 인증 시스템으로 인증되었습니다.
www.redhat.com

관련 링크

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

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