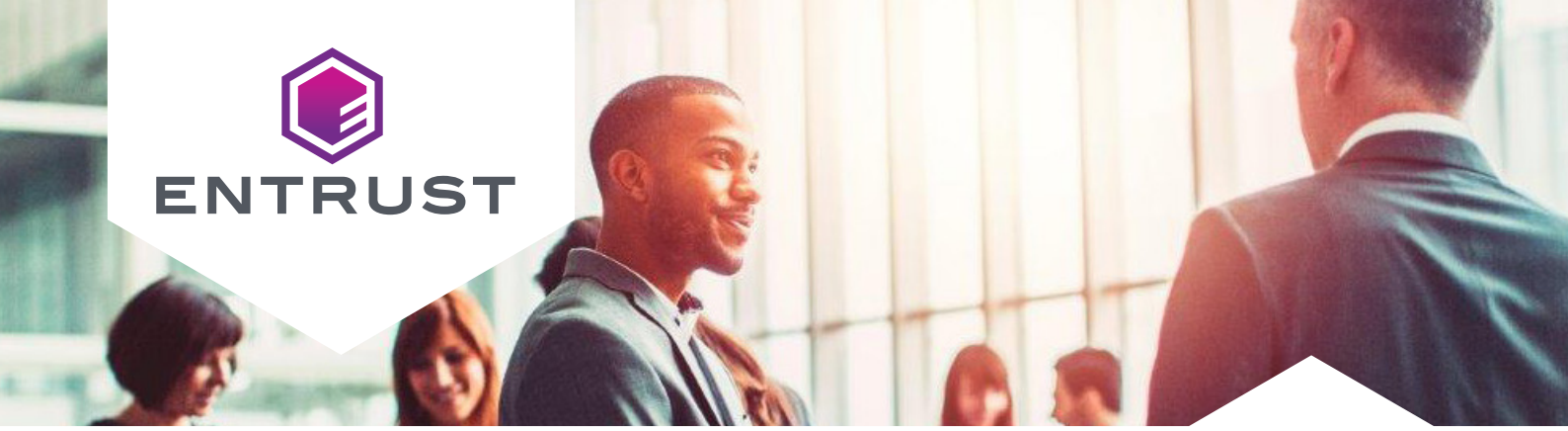


Entrust, 기업 특정 보안 요건을 해결하는 자체 관리형 PKI 솔루션 제공

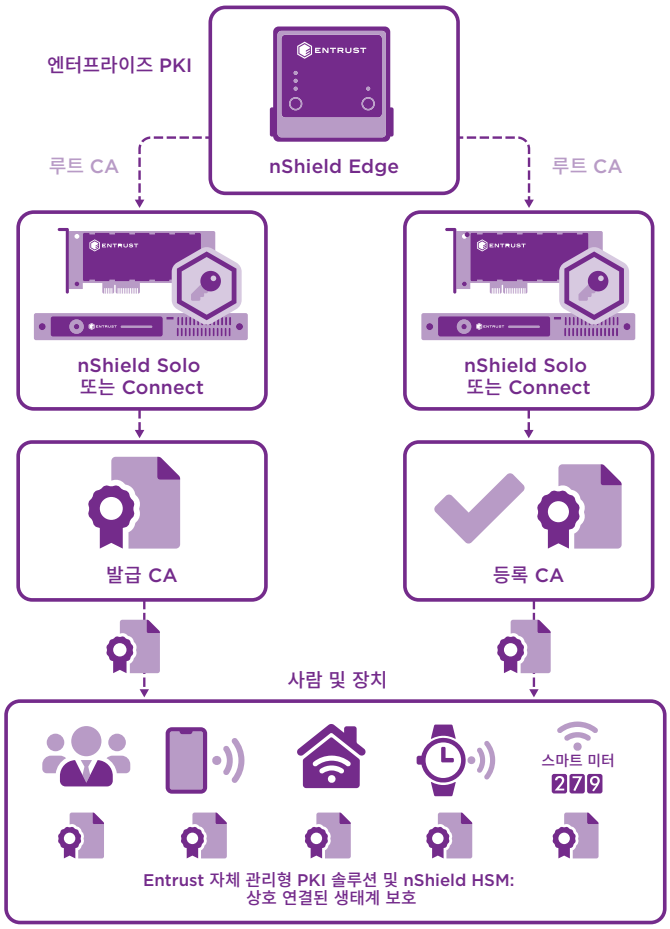
Entrust 서비스와 하드웨어 보안 모듈로안전한 신원 관리 솔루션 배포 및 관리

하이라이트

- 개인과 장치의 신원 보호
- 올바른 절차와 방법 개발
- 기존 PKI 배포 상태 평가
- PKI 마이그레이션으로 확대되는 요건 충족
- 편리한 보안 규정 준수 및 감사 지원

문제점: 상호 연결된 기술의 도입이 증가함에 따라 기존 PKI(공개 키 기반 구조) 성능이 확장되고 새로운 인프라 필요

암호화 지원 애플리케이션의 사용이 증가하고 사물 인터넷(IoT)의 영향으로 PKI에 대한 새로운 요구가 전례없이 발생하고 있습니다. 자격 증명 요건이 커지고 장치와 센서가 가까운 네트워크 생태계에 안전하게 연결되는 방식을 관리해야 하는 필요성이 확대되면서 기업은 기존 PKI 상태를 재평가하게 되었습니다. 변화하는 보안 표준과 함께 기업은 PKI 구축 전략을 재고하고 어떤 경우에는 새롭고 더욱 강력한 배포로 마이그레이션하고 재설계하고 있습니다.



ENTRUST.COM/HSM에서 자세히 보기

기업 특정 보안 요건을 해결하는 자체 관리형 PKI 솔루션

과제: 엔터프라이즈 PKI 전반에 걸쳐 강력한 신뢰점을 유지하여 보안에 더욱 민감한 애플리케이션의 운영 요구 충족

PKI를 사용하며 보안에 더욱 민감한 애플리케이션에서는 개인 키를 보강하는 보안이 필수입니다. 2020년 포네몬 연구소의 PKI 동향 보고서에 따르면 디지털 인증서를 사용하는 상위 3개 애플리케이션은 공용 웹사이트용 SSL/TLS, 공용 클라우드 기반 애플리케이션, 엔터프라이즈 사용자 인증입니다. 디지털 인증서를 사용하면 애플리케이션과 장치를 식별하고 신뢰할 수 있는 생태계에 대한 인증을 수행할 수 있습니다. 이를 위해서는 점차 증가하는 개인 키를 자동화되고 신뢰할 수 있는 방식으로 보호하고 관리할 수 있어야 합니다.

솔루션: 컨설팅 서비스와 올바른 보안 하드웨어를 결합하여 요건 정의에서 배포, 교육에 이르기까지 고객을 지원하는 Entrust 자체 관리형 PKI 제품

기업 PKI 요건은 일반적으로 비즈니스, 클라이언트, 지원하는 애플리케이션에 따라 다릅니다. Entrust 자체 관리형 PKI 제품은 기업 PKI 설계와 구현에 대한 기술적 전문 지식과 시스템에 대한 강력한 신뢰점을 제공하는 데 필요한 보안 하드웨어를 결합합니다. 서비스에는 고객이 현재 요건과 미래 요건을 충족하는 PKI를 배포하는 데 필요한 인프라의 설계 및 구축과 함께 초기 요건 평가, 절차 및 방법 개발을 포함합니다. 컨설팅으로 고가용성과 중복성이 필요한 운영 환경이나 고객이 자체 PKI 기술 세트를 개발하는 데 도움이 되는 실험 환경을 지원할 수 있습니다. 처음으로 PKI를 배포하는 고객의 경우, 보안 하드웨어 지원과 결합된 문서화 및 배포 서비스가 제공됩니다. 기존 PKI 나 확대되고 있는 PKI 배포를 보유한 고객을 위해 보안 하드웨어와 함께 SHA 마이그레이션 서비스를 비롯한 마이그레이션 서비스와 상태 확인을 제공합니다.

Entrust nShield® 하드웨어 보안 모듈(HSM)은 PKI 배포의 보증성을 높입니다. 인증받은 분리 환경에서 개인 키를 보호하고 관리하도록 설계된 Entrust nShield HSM은 표준 CAPI(암호화 애플리케이션 프로그래밍 인터페이스)를 사용하여 Microsoft, Red Hat, Entrust, RSA 및 Insta의 PKI를 지원합니다.

기업 특정 보안 요건을 해결하는 자체 관리형 PKI 솔루션

자체 관리형 PKI와 함께 Entrust HSM을 사용해야 하는 이유

보안이 중요한 애플리케이션과 연결 장치의 배포로 인해 PKI에 대한 수요가 증가하고 있으며 PKI는 도메인 전체에서 발급된 장치 인증서의 루트 CA(인증 기관)와 개인 키뿐만 아니라 등록 과정까지 보호해야 합니다. HSM을 사용해 개인 키를 보호하지 않는 기업 PKI는 장애에 취약하며 잠재적으로는 심각한 결과를 초래할 수 있습니다. HSM은 보안에 중요한 키의 도난과 오용을 방지하고 장애 조치 지원으로 전체 수명주기 관리를 가능하게 하는 강화된 환경을 제공합니다. HSM을 사용하여 인증서 발급을 신원 확인과 승인에 바인딩하는 것은 CA 보안 침해 사례를 통해 얻은 중요한 가르침입니다. FIPS 140-2 레벨 3과 CC 인증 EAL4+ 포함, 엄격한 보안 표준 인증을 받은 Entrust nShield HSM의 성능은 다음과 같습니다.

- 안전한 변조 방지 환경에 루트 CA와 등록 키 보관 가능
- 스마트카드 기반 정책 및 2단계 인증으로 관리자 액세스 관리
- 공공 부문, 금융 서비스, 기업 관련 규제 요건 준수

Entrust

Entrust nShield HSM은 가상화 환경을 포함하여 전사적으로 신원 자격 증명 관리를 단순화하여 기업이 PCI DSS (Payment Card Industry Data Security Standard) 및 PSD2(Payment Services Directive)와 같은 감사 및 규정 준수 요건을 충족하도록 지원합니다. nShield HSM은 고객사의 특수한 요구를 충족하기 위해 다음과 같은 모델로 제공됩니다.

- nShield Edge HSM: 오프라인 루트 CA 및 개발자 애플리케이션을 위한 휴대용 USB 연결 HSM
- nShield Solo / Solo+ / Solo XC HSM: 서버를 위한 임베디드 PCI Express 고성능 HSM
- nShield Connect / Connect+ / Connect XC HSM: 데이터센터를 위한 네트워크 연결 고성능 HSM

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.

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