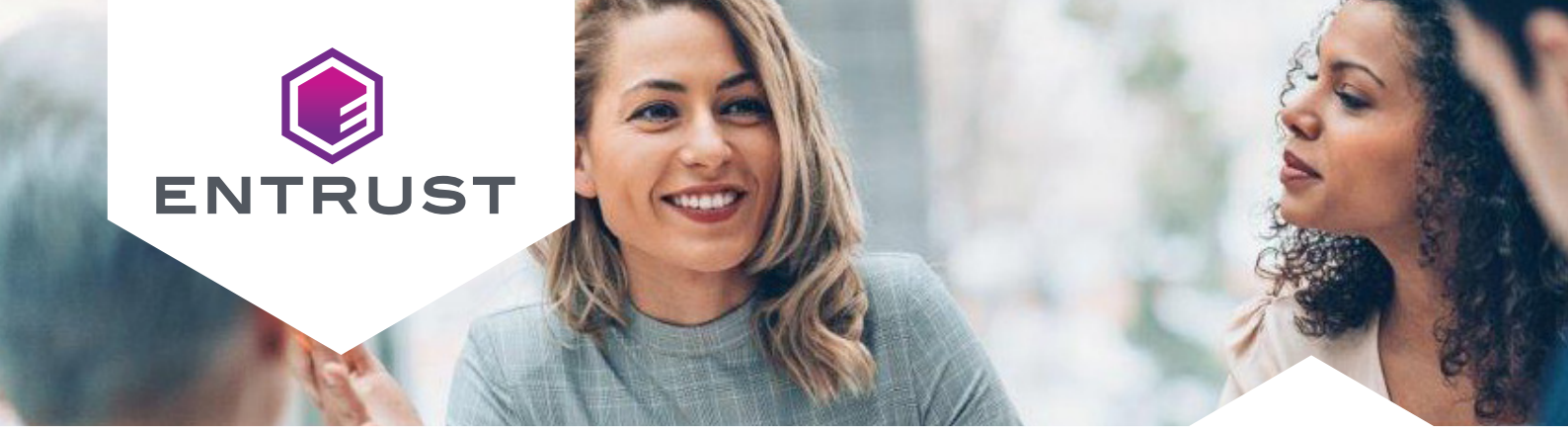


Microsoft와 Entrust, 사물 인터넷의 보안과 신뢰 증진

안전한 IoT 장치 등록을 지원하는 장치 등록 서비스와 하드웨어 보안 모듈

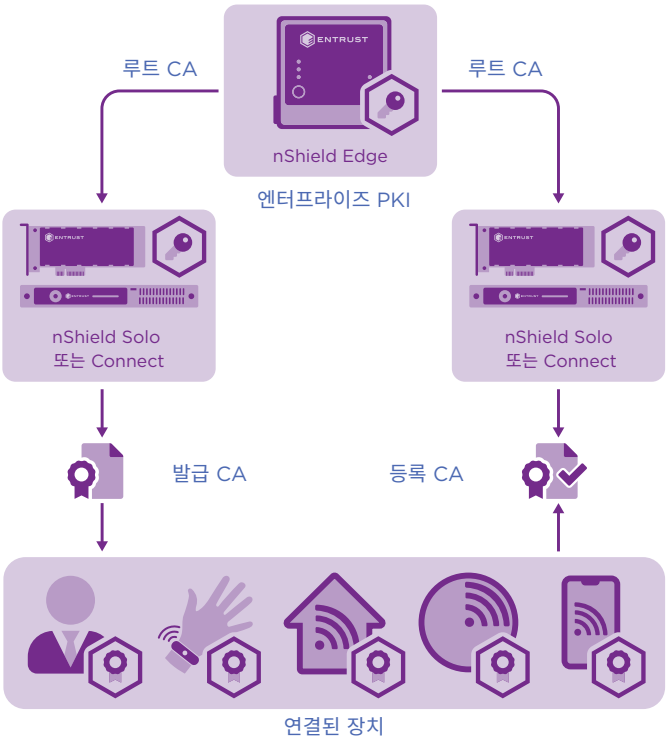
하이라이트

- 네트워크 장치 인증서의무결성 향상
- 기존 PKI를 활용한 장치 등록 지원
- 안전한 키 보관 및 관리 제공
- FIPS 140-2 레벨 3으로 검증받은키 보안 제공
- 편리한 데이터 보안 규정준수

문제: 신원 확인과 인증 목적으로 디지털 인증서를 사용하는 인터넷 연결 네트워크 장치가 늘어나면서 인증서 등록 지원에 대한 필요성 또한 증가

더 많은 장치가 인터넷과 기업 네트워크에 연결되면서 장치 신원 확인과 인증이 매우 중요해졌습니다. 승인되지 않은 장치는 폐쇄된 도메인에 악성 코드를 들여오는 벡터를 생성하여 심각한 위험을 초래할 수 있습니다.

신원 확인과 인증을 위한 장치 자격 증명을 발급하고 관리하기 위해 PKI(공개 키 기반 구조)를 사용하고 있지만, 신뢰할 수 있는 등록 절차 또한 마련되어야 합니다.



Entrust nShield HSM은 엔터프라이즈 PKI 루트와 발급 CA 키를 보호할 뿐만 아니라 장치 인증서를 CA 신뢰점에 바인딩하여 인증서 무결성과 유효성 검사를 실행하는 데 필요한 개인 키도 보호합니다.

ENTRUST.COM/HSM에서 자세히 보기

Microsoft와 Entrust, 사물 인터넷의 보안과 신뢰 증진

과제: 신뢰할 수 있는 도메인 기반 자격 증명을 사용하여 인증서를 안전하게 등록할 수 있는 연결 장치 수 확대 지원

제한된 도메인에 승인된 연결 장치가 점점 더 많아지는 상황에서 장치 인증서 발급은 네트워크 환경의 보안을 구축하는 첫 단추일 뿐입니다. CA(인증 기관)에서 인증서를 등록해야 장치 연결의 유효성을 검사하고 제어할 수 있습니다. 등록 절차를 뒷받침하는 암호키를 보호하고 관리하는 것은 전체 시스템에 대한 신뢰를 제공하는 핵심 기반입니다.

솔루션: Microsoft와 Entrust를 함께 이용하여 연결 장치의 인증서 등록 보안

Microsoft AD CS(Active Directory Certificate Services)의 기능 중 하나인 NDES(Network Device Enrollment Service)는 SCEP(Simple Certificate Enrollment Protocol)를 구현하여 인증서 등록 시 RA(등록 기관)와 연결 장치 간의 통신을 정의합니다. Microsoft Intune과 System Configuration Manager와 같은 클라우드 및 온프레미스 기반 솔루션은 NDES를 사용하여 장치를 프로비저닝하고 등록합니다. NDES를 사용하면 Windows Server에 연결된 장치의 디지털 ID를 상응하는 개인 키에 바인딩하여 등록하고 확인할 수 있습니다. CA를 신뢰점으로 사용하는 이 서비스는 인증서 등록과 신뢰성·무결성 확인을 지원합니다.

로컬 파일로 보관한 키를 사용하여 서버에서 발급 절차를 실행하면 해당 키가 복제, 수정, 치환과 같은 공격에 취약해질 수 있습니다. Entrust nShield 하드웨어 보안 모듈(HSM)은 개인 NDES 키를 보호하여 인증서 등록 절차의 보증도를 높입니다. Entrust nShield® HSM은 Microsoft 표준 CAPI(암호화 애플리케이션 프로그래밍 인터페이스)로 Microsoft NDES와 통합됩니다.

Entrust HSM을 Microsoft NDES와 함께 사용해야 하는 이유

사물 인터넷(IoT)이 증가하고 사물 인터넷을 지원하는 연결 장치의 배포가 늘어나면서, PKI는 도메인 전체에서 발급된 인증서의 보안을 뒷받침하는 루트 CA의 개인 키를 보호할 뿐만 아니라, 증가하는 인증서 등록까지 보호해야 합니다. HSM을 사용해 개인 키를 보호하지 않고, 인증서 등록과 유효성 검사 메커니즘을 사용하지 않는 기업 PKI는 장애에 취약하며 잠재적으로는 심각한 결과를 초래할 수 있습니다. HSM은 보안에 중요한 키 도난과 오용을 방지하고, 전체 수명주기 관리를 가능하게 할 뿐만 아니라 여러 HSM을 사용하여 고가용성을 제공하는 장애 조치 지원으로 강화된 환경을 제공합니다. Entrust nShield HSM을 사용하여 인증서 발급을 신원 확인과 승인에 바인딩하고 인증서 등록과 유효성 검사를 제어하는 것은 CA 보안 침해 사례를 통해 얻은 중요한 가르침입니다.

Microsoft와 Entrust, 사물 인터넷의 보안과 신뢰 증진

FIPS 140-2 레벨 3 포함, 엄격한 보안 표준 인증을 받은 Entrust nShield HSM의 성능은다음과 같습니다.

- 안전한 변조 방지 환경에 루트 CA와 등록 키 보관
- 스마트카드 기반 정책 및2단계 인증으로 관리자 액세스 관리
- 공공 부문, 금융 서비스, 기업 관련 규제 요건 준수

Entrust HSM

Entrust nShield HSM은 Windows Server 2003 출시 이후로 계속해서 AD CS를 지원해왔으며 광범위한 전 세계 고객층에 배포되어왔습니다. NDES 지원은 이 서비스를 확장한 기능입니다. 여러 애플리케이션과 PKI에서 자격 증명 관리를 단순화하여 Hyper-V를 포함한 가상 환경에서 작동할 수 있습니다. Entrust nShield HSM은 PCI DSS(Payment Card Industry Data Security Standard)와 같은 감사 및 규정 준수 충족을 지원하며, 이용 가능한 제품 유형은 다음과 같습니다.

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

Microsoft

Microsoft는 비즈니스 리소스를 공유하는 방식, 신원과 액세스 제어를 관리하는 방식을 혁신했습니다. Microsoft AD CS와 NDES 기반 시스템은 공개 키 인증서를 생성하고 관리하는 맞춤형 서비스를 제공하여 사람과 장치 간에 신뢰할 수 있는 비즈니스 환경을 구축합니다. Microsoft NDES:

- RA로 장치 인증서 프로비저닝 및 등록
- 도메인 기반 자격 증명을 사용하여 등록 보안
- 인증서 유효성 검사 및 폐기 서비스 제공

www.microsoft.com

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