



ENTRUST

# 신뢰할 수 있는 Entrust 신원 솔루션, 디지털 비즈니스 혁신 지원

## 통합 솔루션으로 PKI 배포 보안 강화

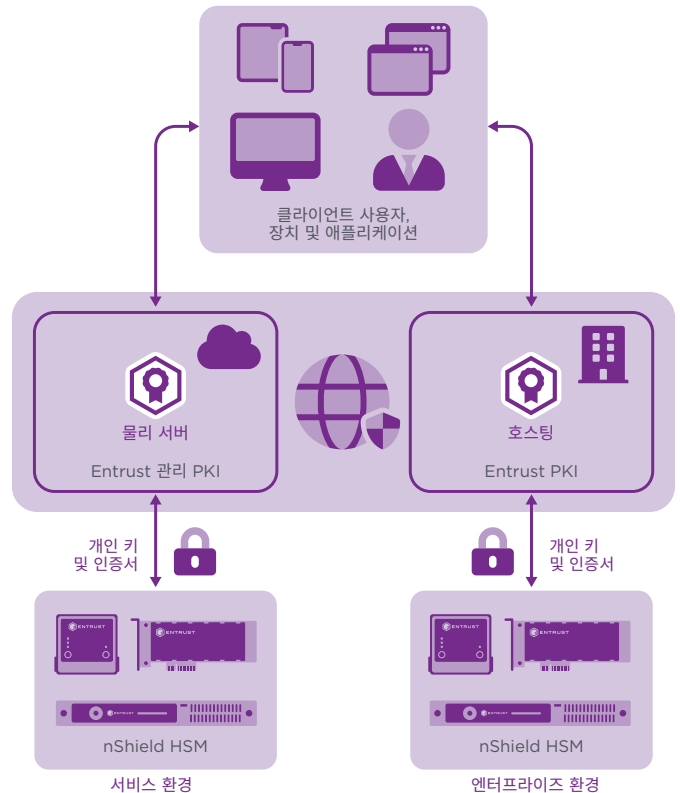
### 하이라이트

- 모든 기업 애플리케이션의 사용자 신원 보호
- 온프레미스 및 호스팅 배포를 대상으로 액세스 제어
- 백업/복구를 포함한 인증서 수명 주기 관리
- 신뢰점을 제공하여 민감한 개인 키 보호
- FIPS 및 CC 인증으로 규정 준수 용이
- 온프레미스, 클라우드, 하이브리드 배포 지원

### 문제점: 빠르게 성장하는 생태계에서 신뢰할 수 있는 신원에 대한 요구 증가

사물 인터넷(IoT), 휴대기기의 급증, 새로이 등장하는 요건들(BYOD, 'Bring Your Own Device' 프로그램과 IoT 연결 장치 등록을 위한 장치 인증서 발급 지원 요건 등)로 강력한 신원 관리가 그 어느 때보다 중요해지고 있습니다. PKI(공개키 기반 구조) 솔루션은 사용자, 장치,

애플리케이션, 서비스를 대상으로 신뢰할 수 있는 신원을 구축하여 기업 핵심 시스템과 리소스에 대한 보안 액세스를 보장하는 데 이상적이며, 이를 통해 보안 환경의 핵심 요소를 갖춰줍니다.



일반적인 원격 관리 배포에 사용하는 구성 요인을 보여주는 도표

# 신뢰할 수 있는 Entrust 신원 솔루션, 디지털 비즈니스 혁신 지원

## 과제: 안전한 CA(인증 기관) 키 관리

온프레미스나 호스팅된 PKI에서 사용하는 개인 키를 안전하게 보호하는 것은 효과적인 보안 전략에 필수적입니다. PKI의 신뢰성은 CA 계층 구조에서 개인 키에 부여하는 보호 수준, 그리고 관련 인증 절차에 달려있습니다. 소프트웨어에서 보관·관리하는 CA 키는 고난도 위협에 취약할 수 있으며 이는 보안 침해로 이어질 수 있습니다. 전용 하드웨어 키 관리는 보안을 강화하고, 신뢰할 수 있는 비즈니스 생태계에 가해지는 위험을 줄여줍니다.

## 솔루션: 강력한 신뢰 기반을 갖춘 통합 솔루션

Entrust PKI 솔루션은 중요한 비즈니스 애플리케이션을 위한 인증서 기반 보안을 구축하고 관리합니다. Entrust Security Manager를 사용하면 고객사가 보유한 디지털 인증서를 자체적으로 배포하고 관리할 수 있습니다. 이 제품은 사용자를 인증하고 액세스를 제어하며 암호화 애플리케이션을 보호합니다. 간접적인 관리 방식을 원하는 고객사는 Entrust 관리형 PKI의 호스팅 솔루션을 이용할 수 있습니다.

Entrust nShield® 하드웨어 보안 모듈(HSM)은 Entrust PKI 제품과 통합되어 민감한 키의 기밀성과 무결성을 보호합니다. 온프레미스나 호스팅된 PKI의 보안을 확대하고자 하는 기업은 nShield HSM, 온프레미스 또는 서비스형 Entrust 솔루션을 배포하여 허가받지 않은 대상에게 중요한 키가 노출되는 것을 방지할 수 있습니다. nShield HSM은 CA 개인 키를 안전하게 생성·저장·관리합니다.

## nShield를 Entrust Security Manager, 관리형 PKI와 함께 사용해야 하는 이유

하드웨어 신뢰점 없이도 PKI를 배포할 수는 있지만, 인증받은 HSM의 암호화 범위 외부에서 처리하는 CA 키는 PKI 자격 증명 발급 기능과 인증서 폐기 기능을 훼손할 수 있는 공격에 훨씬 더 취약합니다.

HSM을 사용하는 것은 PKI 배포의 모범 사례로 널리 간주되며, 검증받고 감사 가능한 방법으로 귀중한 암호화 자료에 대한 보안을 제공합니다.

HSM을 사용하는 기업은 다음과 같은 이점을 누릴 수 있습니다.

- 역할 분리를 시행하는 강력한 액세스 제어 메커니즘을 차용할 뿐만 아니라 신중하게 설계한 암호화 범위 내에서 CA 키를 보호하여 권한을 부여받은 대상에만 키 이용을 허용함
- 정교한 키 관리, 보관, 중복 기능을 활용하여 필요할 때 언제든지 키에 액세스할 수 있도록 가용성 보장
- 까다로운 애플리케이션이 늘어나는 경우에도 지원할 수 있는 우수한 성능 제공

nShield HSM의 Entrust Ready 인증은 상호 운용성과 배포 용이성, 강화된 보안을 보장합니다.

# 신뢰할 수 있는 Entrust 신원 솔루션, 디지털 비즈니스 혁신 지원

Entrust nShield HSM은 민감한 키 자료를 생성·보호·관리하도록 설계된 고성능 암호화 장치입니다. 엄격한 보안 표준 인증을 받은 nShield HSM의 성능:

- 안전한 변조 방지 환경에 키 보관 가능
- 공공 부문, 금융 서비스, 기업 관련 규제 준수
- 행정 업무에서 보안 기능을 분리하여 보안 정책 집행 가능
- 고성능 타원 곡선 암호(ECC) 지원

Entrust nShield HSM은 구체적인 요구 성능과 예산 상황에 맞춰 이용하실 수 있습니다.

- nShield Edge HSM: 저용량의 오프라인 루트 CA 구성을 위한 휴대용 USB 연결 HSM
- nShield Solo+ 및 Solo XC HSM: 서버와 보안 장치를 위한 고성능 임베디드 PCIe HSM
- nShield Connect+ 및 Connect XC HSM: 가용성 높은 환경을 위한 고성능 네트워크 연결 HSM
- 서비스로서의 nShield: 유연하고 비용 효율적인 방법으로 우수한 성능을 제공하는 구독제 서비스

## 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.

## 관련 링크

[entrust.com/HSM](https://entrust.com/HSM)을 방문하면 Entrust nShield HSM에 대해 자세히 알아보실 수 있습니다.

[entrust.com](https://entrust.com)을 방문하면 Entrust의 신원, 접근, 통신, 데이터 관련 디지털 보안 솔루션에 대해 자세히 알아보실 수 있습니다.

Entrust nShield HSM  
관련 정보 확인 및 문의

[HSMinfo@entrust.com](mailto:HSMinfo@entrust.com)  
[entrust.com/HSM](https://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](https://entrust.com/HSM)



ENTRUST