



ENTRUST

# Nexus GO Signing과 Entrust로 강력한 디지털 서명 보안 확보



Enabling trusted identities

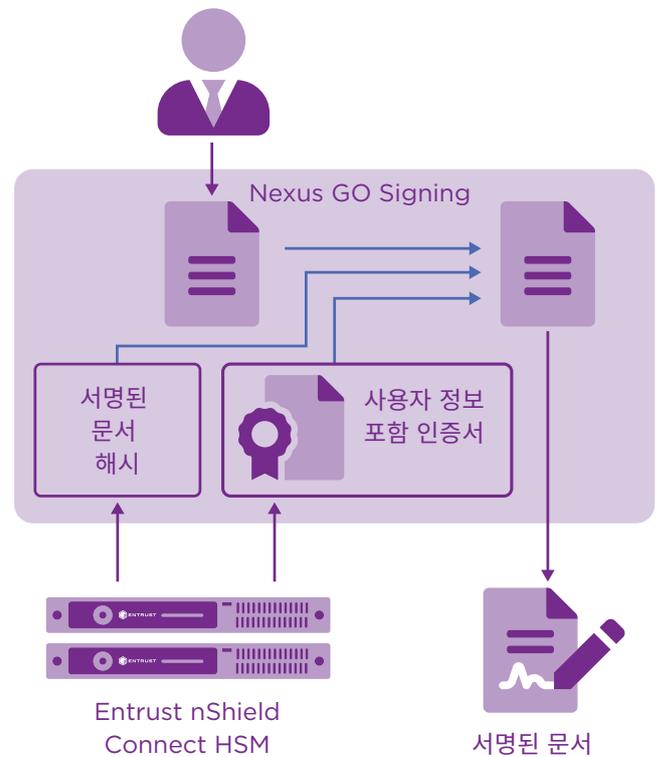
Entrust와 Nexus, 보안성 높은 디지털 서명 서비스 제공

## 하이라이트

- 계약서, 합의서 등 기타 중요한 문서의 조작 방지
- 신뢰할 수 있는 문서 출처 보장
- 신뢰할 수 있는 서명자 신원 설정
- ETSI, eIDAS 등 국가 표준화 기관의 요건 준수
- 계약서와 기타 문서의 종이 사본을 기반으로 수동 프로세스 디지털화 및 자동화

## 문제점: 문서 서명과 관련된 수동 프로세스에서 손쉽게 발생하는 오류

디지털 문서는 강력한 도구이지만 쉽게 수정할 수 있고 출처를 입증하기가 어렵습니다. 대부분의 문서 서명 프로세스는 보안상의 이유로 여전히 수동으로 남아 있습니다(예: 계약 관련 프로세스).



# Nexus GO Signing과 Entrust로 강력한 디지털 서명 보안 확보

## 과제: 보안 위험 없이 디지털 문서 서명 구현

문서 서명은 서명 자격 증명이 조작되지 않고 정확한 서명자 개인에게 안전하게 연결되어 있는지 확인할 수 있어야 합니다. 솔루션을 많은 서명 사례에 적용하려면 eIDAS, ETSI와 같은 규정이나 정부 요건을 준수해야 합니다.

## 솔루션: 하드웨어 보안 모듈(HSM)을 사용하여 신뢰할 수 있는 문서 서명 제공

Nexus GO Signing은 PDF와 XML 문서에서 PAdES/XAdES/eIDAS 사양에 따라 고급 디지털 서명을 생성합니다. 서명은 문서의 콘텐츠를 서명된 해시 및 인증서와 함께 사용자 데이터와 연결하고, 사용자 데이터는 서명자를 서명 자격 증명과 결부시킵니다.

사용자는 강력한 이중 인증으로 서명 절차에 동의합니다. 그 결과는 PAdES/XAdES/eIDAS를 준수하고 업데이트를 보장하며, 서명·서명된 인증서를 포함하는 문서입니다. 여러 사용자가 동일한 문서에 서명할 수 있습니다.

## nShield HSM을 Nexus GO Signing과 함께 사용해야 하는 이유

Entrust nShield Connect HSM은 Nexus GO Signing 및 Nexus CA와 통합되어 키에 논리적·물리적 종합 보호를 제공합니다. 이 통합 솔루션은 감사 가능한 방법으로 보안 정책을 이행하도록 지원합니다.

HSM은 서명 자격 증명의 무결성을 유지하는 데 사용되며, 서명에 사용되는 암호키를 처리하고 사용자를 서명 키에 연결하는 인증서 발급의 신뢰점 역할을 맡습니다.

HSM을 사용하여 서명 자격 증명과 인증서 발급을 처리하는 솔루션으로 중요한 키를 훼손할 수 있는 공격을 더욱 강력하게 방지할 수 있습니다. HSM은 귀중한 암호화 자료를 보호하는 방법으로서 유일하게 검증받았으며 감사 가능한 방법입니다.

Entrust nShield Connect HSM을 통해 Nexus' 고객은 다음 이점을 누릴 수 있습니다.

- 강력한 액세스 제어 메커니즘을 이용하며 세심하게 고안된 암호화 범위 내에서 키를 보호해, 승인된 목적으로만 사용하도록 보장
- RSA와 ECC 알고리즘을 포함하여 까다로운 일회성 서명 키 애플리케이션을 지원하는 우수한 성능 제공

# Nexus GO Signing과 Entrust로 강력한 디지털 서명 보안 확보

Entrust nShield Connect HSM은 암호화 처리, 키 보안, 관리를 안전하게 이행할 수 있도록 강화된 조작 방지 환경을 제공합니다. nShield HSM을 사용하면 다음과 같은 이점을 활용할 수 있습니다.

- 빈틈없이 통제되는 조작 방지 환경을 제공하여 암호키의 안전한 보호와 관리 가능
- 행정 업무에서 보안 기능을 분리하여 키 사용 정책 집행 가능
- 산업 표준 API(PKCS # 11, OpenSSL, JCE, CAPI, CNG, 웹 서비스 API와 nShield 웹서비스 옵션팩 포함)를 사용하는 애플리케이션과의 인터페이스

## 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.

## Nexus Group

스웨덴의 Nexus Group은 혁신적이고 빠르게 성장하는 신원 보안 회사입니다. 물리적 세계와 디지털 세계에서 사람과 사물에 대해 신뢰할 수 있는 신원을 제공하여 사회를 보호합니다. 대부분의 기술은 Nexus Smart ID 솔루션에 통합되어 조직이 물리적 ID와 디지털 ID를 발급·관리하고, 물리적 액세스와 디지털 액세스를 관리하며 전자 서명을 활성화하고, 공개 키 기반 구조(PKI) 인증서를 발급·관리할 수 있도록 표준화되고 사용하기 쉬운 모듈을 제공합니다. Smart ID 솔루션은 기업 ID, 시민 ID, IoT(사물 인터넷) 보안에 가장 일반적으로 사용됩니다. Nexus는 유럽, 인도, 미국 소재 17개 지사에서 일하는 300명의 직원을 두고 있으며, 글로벌 파트너 네트워크를 보유하고 있습니다.

## 관련 링크

[entrust.com/HSM](https://entrust.com/HSM) 또는 [www.nexusgroup.com](https://www.nexusgroup.com)을 방문하면 자세한 기술 사양을 확인하실 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)

