Hochsichere digitale Signaturen mit Nexus GO Signing und Entrust

Enabling trusted identities

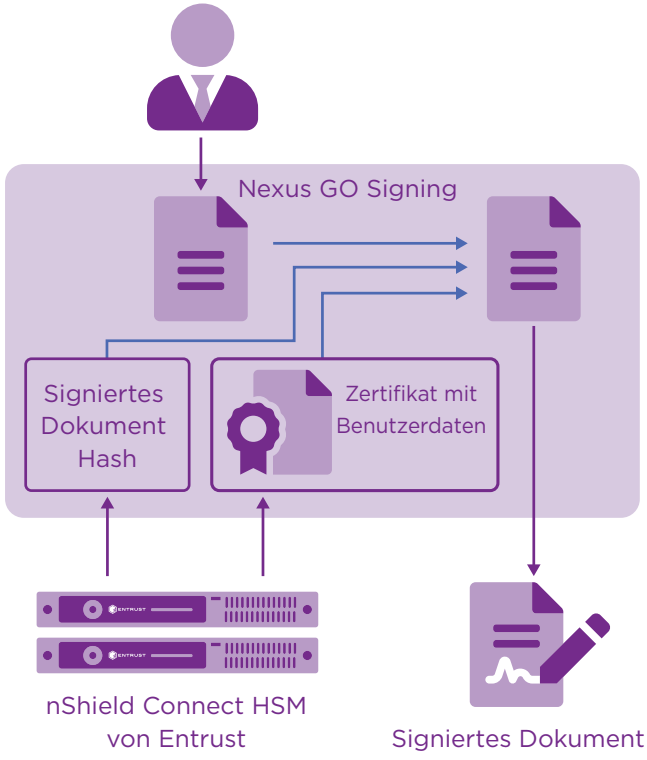
Entrust und Nexus stellen einen äußerst sicheren digitalen Signaturdienst bereit

ECKPUNKTE

- Schutz vor Manipulation von Vereinbarungen, Verträgen und anderen wichtigen Dokumenten
- Gewährleistung einer vertrauenswürdigen Quelle des Dokuments
- Ermittlung der vertrauenswürdigen Identität des Unterzeichners
- Einhaltung der Anforderungen von ETSI, eIDAS und nationalen Standardisierungsgremien
- Digitalisierung und Automatisierung manueller Prozesse, die auf der Papierfassung von Verträgen und anderen Dokumenten beruhen

Die Problemstellung: Manuelle Verfahren mit Dokumentensignatur sind anfällig für Fehler

Digitale Dokumente sind ein leistungsfähiges Werkzeug, aber sie können leicht verändert werden, und es ist schwer, ihre Quelle nachzuweisen. Die Unterzeichnung von Dokumenten geschieht aus Sicherheitsgründen häufig immer noch manuell, z.B. wenn es um Verträge geht.



WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Hochsichere digitale Signaturen mit Nexus GO Signing und Entrust

Die Herausforderung: Umsetzung einer digitalen Dokumentensignatur ohne Gefährdung der Sicherheit

Bei der Unterzeichnung von Dokumenten muss sichergestellt werden, dass die Berechtigungsnachweise für Signaturen nicht manipuliert werden und sicher an die richtige Person als Unterzeichner gebunden sind. Damit die Lösung auf viele Unterzeichnungsfälle anwendbar ist, muss sie Vorschriften wie eIDAS und ETSI sowie nationale Anforderungen erfüllen.

Die Lösung: vertrauenswürdige Dokumentensignatur mit Hardware-Sicherheitsmodulen (HSM)

Nexus GO Signing generiert komplexe digitale Signaturen gemäß den PAdES/XAdES/eIDAS-Spezifikationen auf PDF- und XML-Dokumenten. Die Signatur verknüpft den Inhalt des Dokuments sowie einen signierten Hash und ein Zertifikat mit den Benutzerdaten, was wiederum den Unterzeichner mit den entsprechenden Berechtigungsnachweisen verknüpft.

Der Benutzer gibt seine Zustimmung zum Signaturverfahren mit starker Zwei-Faktor-Authentifizierung. Das Ergebnis ist ein Dokument, das PAdES/XAdES/eIDAS-konform, für die Aktualisierung gesperrt und mit einer eingefügten Signatur und einem signierten Zertifikat versehen ist. Mehrere Benutzer können dasselbe Dokument unterschreiben.

Warum nShield HSM mit Nexus GO Signing?

nShield Connect HSM von Entrust lassen sich mit Nexus GO Signing und der Nexus CA integrieren, um einen umfassenden logischen und physischen Schutz der Schlüssel zu gewährleisten. Die Kombination liefert eine überprüfbare Methode zur Durchsetzung von Sicherheitsrichtlinien.

Das HSM wird verwendet, um die Integrität der Berechtigungsnachweise für die Signatur zu erhalten: Es verwaltet die kryptographischen Schlüssel, die zum Signieren verwendet werden, und er der Vertrauensanker für die Ausstellung von Zertifikaten, die den Benutzer und die Signaturschlüssel verknüpfen.

Durch die Handhabung von Berechtigungsnachweisen für Signaturen und der Ausstellung von Zertifikaten mit einem HSM wird die Lösung deutlich widerstandsfähiger gegen Angriffe, die kritische Schlüssel kompromittieren können. HSM sind der einzige nachgewiesene und prüfbare Weg, um wertvolles kryptographisches Material zu sichern.

nShield Connect HSM von Entrust ermöglichen Nexus-Kunden:

- Schlüssel innerhalb sorgfältig konzipierter kryptographischer Grenzen zu sichern. Eine robuste Zugriffskontrolle sorgt dafür, dass die Schlüssel ausschließlich zu den autorisierten Zwecken verwendet werden.
- Überragende Leistung bei der Unterstützung anspruchsvoller Anwendungen mit Einmal-Signierung, einschließlich RSA- und ECC-Algorithmen zu bieten.

Hochsichere digitale Signaturen mit Nexus GO Signing und Entrust

- nShield Connect HSM von Entrust bieten eine gefestigte, manipulationssichere Umgebung für sichere kryptographische Verarbeitung, Schlüsselschutz und Schlüsselverwaltung. Mit nShield HSM können Sie:

- eine streng kontrollierte, manipulationssichere Umgebung für die sichere Verwahrung und Verwaltung von Kodierungsschlüsseln bereitstellen

- Richtlinien zur Verwendung von Schlüsseln durchsetzen und dabei Sicherheitsfunktionen von Verwaltungsaufgaben trennen

- Anwendungen über branchenführende API (PKCS#11, OpenSSL, JCE, CAPI, CNG, nCore und nShield Web Services Crypto API) anbinden

HSM von Entrust

nShield HSM von Entrust gehören zu den leistungsstärksten, sichersten und am einfachsten integrierbaren HSM-Lösungen am Markt. So erleichtern sie die Einhaltung regulatorischer Vorschriften und bieten höchste Daten- und Anwendungssicherheit für Unternehmen sowie Finanz- und Regierungsbehörden. Unsere einzigartige Security World-Architektur für die Schlüsselverwaltung bietet starke, granulare Schlüsselkontrollen hinsichtlich Zugriff und Nutzung.

Nexus Group

Die schwedische Nexus-Gruppe ist ein innovatives und schnell wachsendes Identitäts- und Sicherheitsunternehmen. Es schützt die Öffentlichkeit, indem es Menschen und Gütern in der physischen und digitalen Welt vertrauenswürdige Identitäten verleiht. Der Großteil der Technologie ist in die Nexus Smart ID-Lösung integriert, die standardisierte und benutzerfreundliche Module bietet, mit denen Unternehmen physische und digitale IDs ausstellen und verwalten, den physischen und digitalen Zugang verwalten, elektronische Signaturen ermöglichen und PKI-Zertifikate (Public Key Infrastructure) ausstellen und verwalten können. Die Smart-ID-Lösung wird am häufigsten für Unternehmens-IDs, Personen-IDs und IoT-Sicherheit (Internet der Dinge) verwendet. Nexus hat 300 Mitarbeiter in 17 Büros in Europa, Indien und den USA sowie ein globales Partnernetzwerk.

Weitere Informationen

Detailliertere technische Spezifikationen finden Sie auf **entrust.com/HSM** oder **www.nexusgroup.com**

Mehr Informationen zu Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ÜBER ENTRUST CORPORATION

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

Kontakt:
HSMinfo@entrust.com