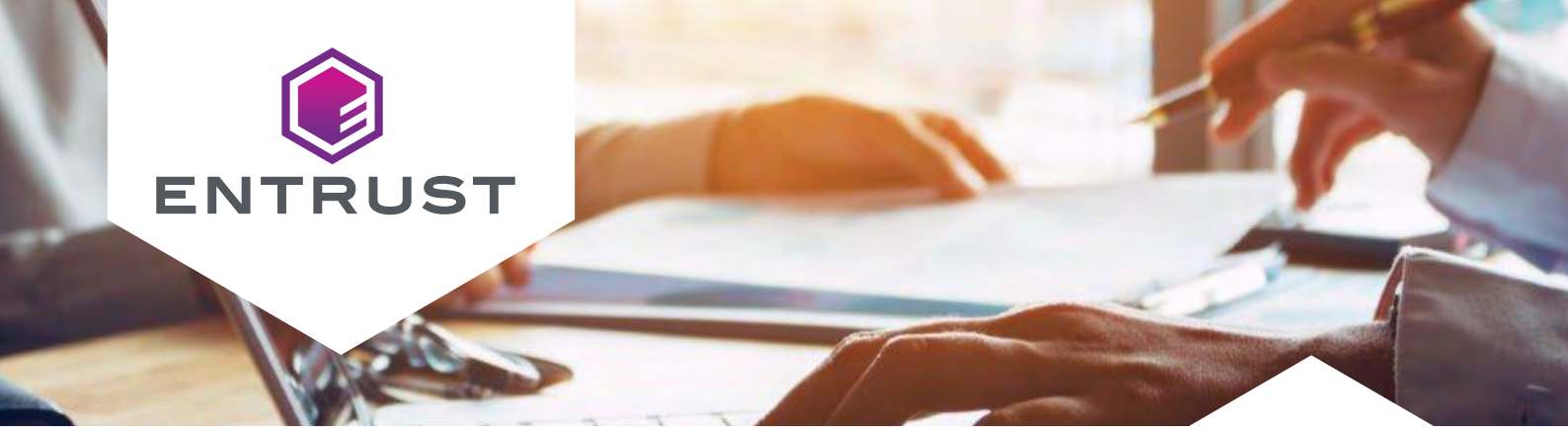


Sichere Public Key Infrastructure mit nShield HSM von Entrust

STRATEGIC TECHNOLOGY PARTNER PROGRAM

Hohes Schutzniveau für PKI-Schlüssel

ECKPUNKTE

- Schutz kritischer Root- und CA-Schlüssel in einem manipulationssicheren, gemäß FIPS 140-2 Level 3 zertifizierten HSM
- Leistungsstarke Authentifizierung für verbundene Geräte
- Einfache Prüfung und Einhaltung von Datensicherheitsvorschriften
- Mehr Datensicherheit und Vertrauen
- Hohes Serviceniveau und wirtschaftliche Agilität

CA: Zertifizierungsstelle VA: Validierungsstelle RA: Registrierungsstelle

Die Herausforderung:

Die Digitalisierung von Unternehmen und das aufkommende Internet der Dinge (Internet of Things, IoT) verdeutlichen, dass für Benutzer, Geräte und Anwendungen, die auf Systeme und Daten zugreifen, verlässliche Identitäten geschaffen werden müssen. Eindeutige und zurückverfolgbare Identitäten für Benutzer und Geräte ermöglichen höhere Einnahmen und Kostensenkungen durch neue Produkte, Dienstleistungen und Geschäftsmöglichkeiten.

Sichere Public Key Infrastructure mit nShield HSM

Um diese Möglichkeiten zu nutzen und Systeme und Daten zu schützen, sollte sichergestellt werden, dass:

- die Benutzer, die das Gerät oder System verwalten, dazu berechtigt sind
- der auf den verbundenen Geräten laufende Code - einschließlich Firmware, Betriebssystem und Anwendungen - zuverlässig ist und nicht verändert wurde
- Daten, die zwischen Geräten, Personen und Anwendungen übertragen werden, gültig und vor unbefugten Änderungen geschützt sind
- finanzielle Transaktionen gesichert und authentifiziert werden können

Eine Public-Key-Infrastruktur (PKI) bietet einen Mechanismus, mit dem authentische Identitäten für Benutzer und Geräte - auch Entitäten genannt - eingerichtet und verwaltet werden können. Nach der Authentifizierung können diese Entitäten auf kritische Unternehmenssysteme und -ressourcen zugreifen und digitale Signierungsvorgänge durchführen. PKIs beruhen auf digitalen Zertifikaten, die von einer Zertifizierungsstelle (CA) signiert sind und die einen öffentlichen Schlüssel an einen bestimmten Benutzer oder ein bestimmtes Gerät binden. Deshalb sind der Root-Schlüssel und der ausstellende private CA-Schlüssel lohnende Ziele für Angreifer. Sie benötigen umfassenden Schutz, da sie sprichwörtlich alle Türen öffnen.

Die Lösung: PKI mit nShield HSM von Entrust

Obwohl es möglich ist, PKIs ohne einen Hardware Root of Trust einzusetzen, können CA-Schlüssel, die außerhalb der kryptographischen Grenzen eines zertifizierten Hardware-Sicherheitsmoduls (HSM) verwaltet werden, anfällig für Angriffe sein. Sie können die Funktionen von PKIs zur Ausstellung von Berechtigungsnachweisen und zum Widerruf von Zertifikaten beeinträchtigen.

Die Verwendung von HSM ist ein anerkanntes und bewährtes Verfahren zum Schutz des Stammverzeichnisses und zur Ausgabe privater CA-Schlüssel, die die Grundlage für PKI-Implementierungen bilden.

nShield® HSM von Entrust können in die Lösungen führender PKI-Anbieter integriert werden. Sie bieten gemäß FIPS 140-2 Level 3 und Common Criteria EAL 4+ zertifizierten Schutz für die privaten Root- und CA-Schlüssel. Kunden genießen erhöhte Sicherheit und können somit die Einhaltung von Anforderungen wie dem Payment Card Industry Data Security Standard nachweisen.

Was nShield besonders macht

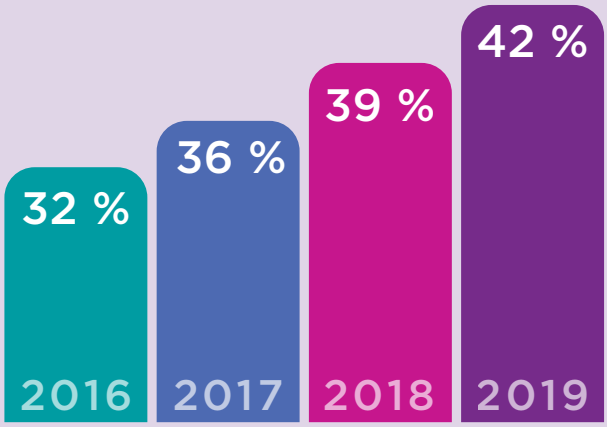
nShield HSM von Entrust bieten eine bewährte und prüfbare Möglichkeit zur Sicherung wertvoller kryptographischer Schlüssel und Materialien. Nach FIPS und Common Criteria zertifizierte nShield HSM:

- sichern Schlüssel innerhalb sorgfältig ausgelegter kryptographischer Grenzen
- wenden robuste Zugangskontrollen an und setzen Aufgabentrennung durch, um sicherzustellen, dass Schlüssel nur von autorisierten Entitäten verwendet werden
- gewährleisten die Verfügbarkeit von Schlüsseln durch den Einsatz ausgeklügelter Schlüsselverwaltungs-, Speicher- und Redundanzfunktionen
- bieten hohe Leistung zur Unterstützung einer wachsenden Zahl anspruchsvoller Anwendungen
- sind skalierbar und somit leichter zu verwalten, so dass Anforderungen besser erfüllt werden können

nShield HSM von Entrust sind in verschiedenen Formfaktoren erhältlich, während nShield as a Service einen abonnementbasierten Zugang zu nShield-Connect-HSM bietet.

Sichere Public Key Infrastructure mit nShield HSM

Wie verwalten Sie die privaten Schlüssel für Ihre Root-, Policy- und ausstellenden CAs?



Hardware-Sicherheitsmodule (HSM)

Quelle: Globale PKI-Trendstudie 2019, Ponemon Institut und Entrust

„Die PKIs von Unternehmen unterstützen im Schnitt 8,5 verschiedene Anwendungen. Das zeigt, dass die PKI zentraler Bestandteil des IT-Rückgrats eines Unternehmens ist“.

Globale PKI-Trendstudie 2019, Ponemon Institut und Entrust

nFinity Partner

nShield HSM von Entrust sind über unser Partnerprogramm nFinity Technology mit den folgenden PKI-Anbietern integriert. Die aktuelle Liste unserer Partner finden Sie auf unserer Website.

axway
KEYFACTOR
cybertronixx
Microsoft
nexus
DEVICE AUTHORITY
IoT Security Simplified
PrimeKey
digicert®
Red Hat
Entrust Datacard
RSA SECURITY™
HID
HID CORPORATION
SAFELAYER
INSTA
TRUSTONIC
Information Security CORPORATION

Weitere Informationen

Mehr Informationen zu den nShield HSMs von Entrust finden Sie auf **entrust.com/HSM**. Auf **entrust.com** erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.

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