Die vertrauenswürdigen Identitätslösungen von Entrust unterstützen die digitale Transformation Ihres Unternehmens

Integrierte Lösungen optimieren die Sicherheit von PKI-Bereitstellungen

ECKPUNKTE

- Sichere Benutzeridentitäten für alle Unternehmensanwendungen
- Kontrollierter Zugriff auf lokale und gehostete Bereitstellungen
- Verwaltung der Zertifikate über ihren gesamten Lebenszyklus einschließlich Sicherung und Wiederherstellung
- Bereitstellung eines Vertrauensankers zum Schutz sensibler privater Schlüssel
- Einhaltung der FIPS- und Common-Criteria-Normen
- Unterstützung von On-Premises-, Cloud- und hybriden Bereitstellungen

Die Problemstellung: zunehmender Bedarf an vertrauenswürdigen Identitäten in einem sich rasant erweiternden Ökosystem

Das Internet der Dinge (Internet of Things, IoT), die ausufernde Verbreitung von Mobilgeräten und immer neue Anforderungen – wie unter anderem bei der Ausstellung von Gerätezertifikaten für Bring Your Own Device Programme (BYOD) sowie der Einführung von IoT-Geräten – haben dazu geführt, dass ein starkes Identitätsmanagement wichtiger ist als jemals zuvor. Public-Key-Infrastructure-Lösungen

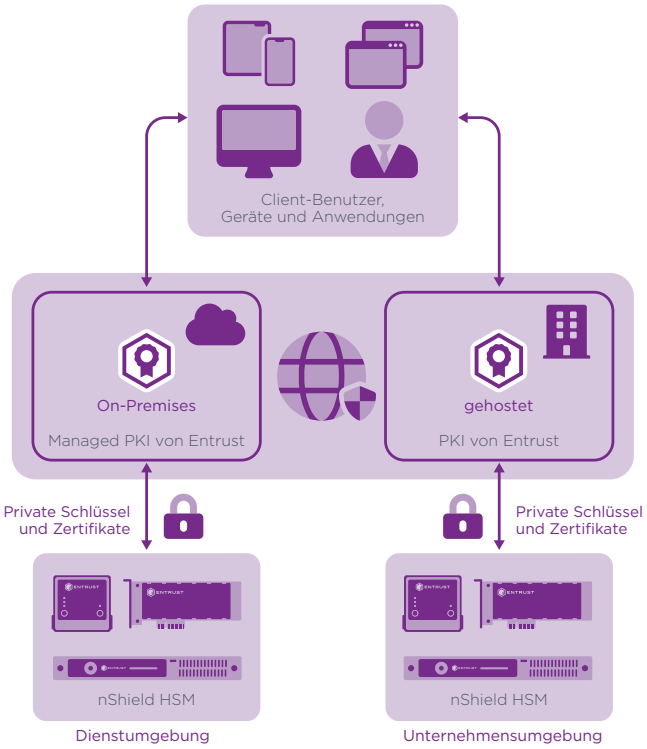

Abbildung 1. verwendeten Komponenten

Die vertrauenswürdigen Identitätslösungen von Entrust unterstützen die digitale Transformationen Ihres Unternehmens

(PKI) eignen sich perfekt, um vertrauenswürdige Benutzer-, Geräte-, Anwendungs- und Dienstidentitäten für den sicheren Zugriff auf Unternehmenssysteme und -ressourcen einzurichten und sind wichtiger Bestandteil einer sicheren Umgebung.

Die Problemstellung: die sichere Verwaltung der Schlüssel der Zertifizierungsstelle (CA)

Starker Schutz der von lokalen oder gehosteten PKI genutzten Schlüssel ist ein wichtiger Bestandteil einer effektiven Sicherheitsstrategie. Wie vertrauenswürdig eine PKI ist, hängt davon ab, inwieweit die privaten Schlüssel in der CA-Hierarchie geschützt sind und entsprechende Überprüfungsverfahren angewandt werden. Werden die CA-Schlüssel in Software gespeichert und verwaltet, sind sie anfällig für komplexe Bedrohungen, die ihre Sicherheit gefährden können. Die entsprechende Verwaltung von Hardware-Schlüsseln verbessert die Sicherheit und reduziert das Risiko innerhalb eines vertrauenswürdigen Unternehmensökosystems.

Die Lösung: eine integrierte Lösung mit einem robusten Vertrauensanker

Die PKI-Lösungen von Entrust bieten zertifizierte Sicherheit für wichtige Unternehmensanwendungen. Der Security Manager von Entrust ermöglicht es Kunden, Ihre eigenen digitalen Zertifikate bereitzustellen und zu verwalten. Das Produkt authentifiziert die Benutzer, kontrolliert den Zugriff und sichert kryptographische Anwendungen. Für Kunden, die sich einen einfachen Lösungsansatz mit wenig Aufwand wünschen, bietet Entrust Managed PKI eine gehostete Lösung.

Die PKI-Lösungen von Entrust sind mit nShield® HSM integriert, um die Vertraulichkeit und Integrität sensibler Schlüssel zu schützen. Unternehmen, die die Sicherheit lokaler oder gehosteter PKI erweitern möchten, können die Lösungen von Entrust mit nShield HSM on-premises oder as-a-Service bereitstellen. So ist garantiert, dass wichtige Schlüssel unter keinen Umständen nicht autorisierten Entitäten offengelegt werden. Die nShield HSM erstellen, speichern und verwalten private CA-Schlüssel sicher.

Warum nShield mit Security Manager und Managed PKI von Entrust?

Obwohl es möglich ist, PKIs ohne einen Hardware-Vertrauensanker einzusetzen, können CA-Schlüssel, die außerhalb der kryptographischen Grenze eines zertifizierten HSM verwendet werden, anfällig für Angriffe sein. Diese können die Funktionen von PKIs zur Ausstellung von Berechtigungsnachweisen und zum Widerruf von Zertifikaten beeinträchtigen.

Die Nutzung von HSM gilt gemeinhin als bewährtes Verfahren für PKI-Bereitstellungen und ist eine erprobte und prüfbare Möglichkeit, wertvolles kryptographisches Material zu sichern. Mithilfe von HSM können Unternehmen:

- CA-Schlüssel innerhalb sorgfältig ausgelegter kryptographischer Grenzen sichern, die robuste Zugangskontrollmechanismen mit erzwungener Aufgabentrennung nutzen, um sicherzustellen, dass Schlüssel nur von autorisierten Entitäten verwendet werden
- durch ausgereifte Management-, Speicher- und Redundanzfunktionen die Verfügbarkeit von Schlüsseln gewährleisten. So ist garantiert, dass bei Bedarf jederzeit darauf zugegriffen werden kann
- hohe Leistung zur Unterstützung einer wachsenden Zahl anspruchsvoller Anwendungen bereitstellen

Das Ready-Zertifikat der nShield HSM von Entrust gewährleistet Kompatibilität, einfache Bereitstellung und optimierte Sicherheit.

Die vertrauenswürdigen Identitätslösungen von Entrust unterstützen die digitale Transformationen Ihres Unternehmens

nShield HSM von Entrust sind leistungsstarke kryptographische Geräte zur Erstellung, Verwaltung und zum Schutz sensiblen Schlüsselmaterials. nShield HSM sind gemäß strenger Normen zertifiziert und:

- speichern Schlüssel in einer geschützten und manipulationssicheren Umgebung
- halten die regulatorischen Anforderungen für den öffentlichen Sektor, Finanzdienstleistungen und Unternehmen ein
- setzen Sicherheitsrichtlinien, die Trennung von Sicherheitsfunktionen und Verwaltungsaufgaben um.
- unterstützen leistungsstarke Elliptic Curve Cryptography (ECC)

nShield HSM von Entrust sind für unterschiedliche Leistungs- und Budgetanforderungen verfügbar:

- nShield Edge HSM: portables HSM mit USB-Anschluss für Offline-Root-CA-Konfigurationen mit geringem Transaktionsvolumen
- nShield Solo+ und Solo XC HSM: leistungsstarke, eingebettete PCIe-HSM für Server und Sicherheitsanwendungen
- nShield Connect+ und Connect XC-HSM: leistungsstarke, netzwerkgebundene HSM für hochverfügbare Umgebungen
- nShield as a Service: abonnement-basierte, leistungsstarke, kostengünstige und flexible Option

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 Kontrolle über den Zugriff auf und die Nutzung von Schlüsseln.

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