Entrust entwickelt selbstverwaltete PKI-Lösungen für unternehmensspezifische Sicherheitsanforderungen

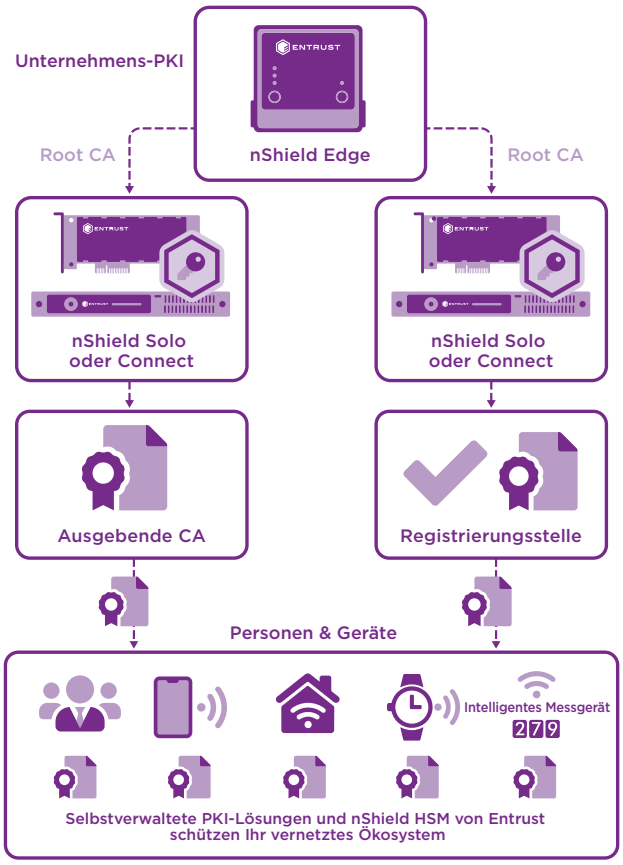
Bereitstellung und Wartung von sicheren Identitätsmanagement-Lösungen mit Diensten und Hardware-Sicherheitsmodulen von Entrust

ECKPUNKTE

- Identitätsschutz von Personen und Geräten
- Entwicklung von korrekten Prozessen und Verfahren
- Zustandsanalyse von bestehenden PKI-Anwendungen
- Migration von PKIs für erweiterte Anforderungen
- Einfachere Sicherheitsaudits und Compliance

Die Problemstellung: Die zunehmende Verbreitung vernetzter Technologien bringt die Kapazitäten bestehender öffentlicher Schlüsselinfrastrukturen (PKI) an ihre Grenzen. Daher sind neue PKI dringender denn je erforderlich.

Die zunehmende Verbreitung vernetzter Technologien und die Auswirkungen des Internet der Dinge (IoT) stellen neue Anforderungen an PKIs. Die Vorgaben für Berechtigungsnachweise nehmen stetig zu und Unternehmen sind mehr und mehr gezwungen, die sichere Vernetzung von Geräten und Sensoren in geschlossenen Netzwerk-Ökosystemen zu verwalten. Daher ist es nötig, dass sie den Zustand ihrer bestehenden PKI evaluieren. Angesichts sich ändernder Sicherheitsstandards überdenken Unternehmen ihre PKI-Implementierungsstrategien. In einigen Fällen entscheiden sie sich für eine Neuentwicklung und migrieren zu anderen, robusteren Implementierungen.



WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Selbstverwaltete PKI-Lösungen für unternehmensspezifische Sicherheitsanforderungen

Die Herausforderung: Unterhaltung eines starken Vertrauensankers für die PKI des gesamten Unternehmens, der die Betriebsanforderung sicherheitsempfindlicher Anwendungen erfüllt.

Weil immer mehr sicherheitsempfindliche Anwendungen PKIs verwenden, ist die Sicherheit privater Schlüssel von entscheidender Bedeutung. Laut der PKI Trendstudie 2020 des Ponemon Institute gehören zu den drei wichtigsten Anwendungen, die digitale Zertifikate verwenden, SSL/TLS für öffentlich zugängliche Websites, öffentliche cloudbasierte Anwendungen und die Authentifizierung von Benutzern innerhalb des Unternehmens. Digitale Zertifikate ermöglichen die Identifizierung von Anwendungen und Geräten und die Authentifizierung in vertrauenswürdigen Ökosystemen. Dies erfordert den Schutz und die Verwaltung einer wachsenden Zahl privater Schlüssel auf automatisierte und vertrauenswürdige Weise.

Die Lösung: Die selbstverwalteten PKI von Entrust kombinieren Beratungsdienste mit der passenden Sicherheitshardware, mit denen der Kunde von der Anforderungsdefinition bis hin zur Bereitstellung und Schulung unterstützt wird.

Die Anforderungen eines Unternehmens an die PKI sind in der Regel je nach Geschäftsfeld, Kunden und unterstützten Anwendungen individuell unterschiedlich. Die selbstverwalteten PKI-Lösungen von Entrust kombinieren technisches Fachwissen zu Auslegung und die Implementierung von Unternehmens-PKIs mit der erforderlichen Sicherheitshardware, um eine solide Vertrauensbasis für das System zu schaffen. Zu den Dienstleistungen gehören die anfängliche Bewertung der Anforderungen und die Entwicklung von Prozessen und Verfahren sowie der Entwurf und die Implementierung der erforderlichen Infrastruktur, um sicherzustellen, dass die Kunden PKIs bereitstellen können, die den aktuellen und zukünftigen Anforderungen entsprechen. Entrust bietet Beratung für operative Umgebungen, die hohe Verfügbarkeit und Redundanz erfordern, oder Laborumgebungen, um Kunden bei der Entwicklung ihrer eigenen PKI-Fähigkeiten zu unterstützen. Für Kunden, die PKIs zum ersten Mal einsetzen, werden Dokumentations- und Bereitstellungsdienste in Kombination mit unterstützender Sicherheitshardware angeboten. Für Kunden mit bestehenden und wachsenden PKI-Implementierungen umfasst das Angebot Integritätsprüfungen und Migrationsdienste, einschließlich SHA-Migrationsdienst sowie Sicherheitshardware.

nShield-Hardware-Sicherheitsmodule (HSM) von Entrust erhöhen die Zuverlässigkeit von PKI-Implementierungen. Die nShield HSM von Entrust wurden für den Schutz und die Verwaltung der zugrunde liegenden privaten Schlüssel in einer zertifizierten isolierten Umgebung entwickelt und unterstützen PKIs von Microsoft, Red Hat, Entrust, RSA und Insta unter Verwendung von standardmäßigen kryptographischen Anwendungsprogrammierschnittstellen (CAPIs).

Selbstverwaltete PKI-Lösungen für unternehmensspezifische Sicherheitsanforderungen

Warum HSM von Entrust mit selbstverwalteter PKI

Der Einsatz sicherheitskritischerer Anwendungen und angeschlossener Geräte stellt erhöhte Anforderungen an PKIs, da erwartet wird, dass sie nicht nur die privaten Schlüssel der Root Certificate Authority (CA) von individuellen Zertifikaten und Gerätezertifikaten, die domänenübergreifend ausgestellt werden, schützen, sondern auch deren Registrierung. Organisatorische PKIs, die keine HSMs zum Schutz ihrer privaten Schlüssel verwenden, sind anfällig für Störungen mit möglicherweise schwerwiegenden Folgen. HSMs bieten eine robuste Umgebung, die sicherheitskritische Schlüssel vor Verlust und Missbrauch schützt, und ihre volle Lebenszyklusverwaltung mit Failover-Unterstützung ermöglicht. Die Bindung der Zertifikatsausstellung an Identitätsprüfungen und Genehmigungen unter Verwendung eines HSM war eine wichtige Lektion, die man aus den CA-Sicherheitslücken gelernt hat. nShield HSM von Entrust sind nach strengen Sicherheitsstandards einschließlich FIPS 140-2 Level 3 und Common Criteria EAL 4+ zertifiziert und:

- speichern Root-CA und Registrierungsschlüssel in einer sicheren und manipulationssicheren Umgebung
- verwalten den Administratorzugriff mit Smartcard-basierten Richtlinien und Zwei-Faktor-Authentifizierung
- halten die regulatorischen Anforderungen für den öffentlichen Sektor, Finanzdienstleistungen und Unternehmen ein

Entrust

nShield HSM von Entrust vereinfachen die Verwaltung von Identitätsnachweisen im gesamten Unternehmen, einschließlich virtualisierter Umgebungen. Sie erleichtern Unternehmen die Erfüllung von Audit- und Compliance-Anforderungen wie dem Payment Card Industry Data Security Standard (PCI DSS) und der Zahlungsdiensterichtlinie PSD2. HSM von Entrust sind in den folgenden Ausführungen erhältlich, um spezifische Kundenanforderungen zu erfüllen:

- nShield Edge HSM portables HSM mit USB-Anschluss für Offline-Root-CAs und für Entwickleranwendungen
- nShield Solo XC HSM (+ models are End Of Sale) integriertes PCI-Express-Hochleistungs-HSM für Server
- nShield Connect XC HSM netzwerkgebundenes Hochleistungs-HSM für Rechenzentren

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

ENTRUST

Kontakt:
HSMinfo@entrust.com