Optimierte Sicherheit: hochsicherer Schlüsselschutz von Entrust für Red Hat Certificate System

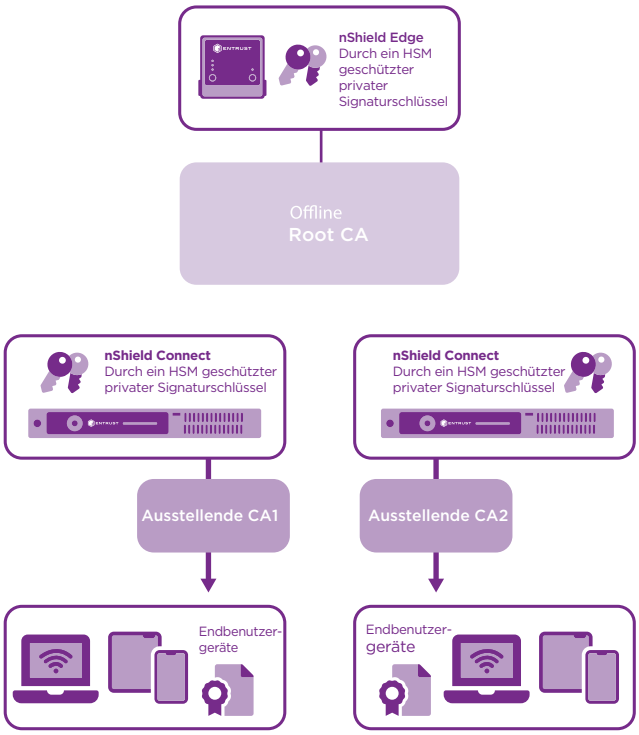
Vertrauen in Public Key Infrastructure (PKI) aufbauen

ECKPUNKTE

- Erweiterte Sicherheit des Red Hat Certificate Systems für Anwendungen mit dem Commercial-Solutions for-Classified-Zertifikat (CSfC-Zertifikat) der NSA
- Verstärkter Sicherheitsrahmen für die Verwaltung von Benutzeridentitäten und die Wahrung der Vertraulichkeit der Kommunikation
- Schutz von Transaktionen und PKI-fähigen Anwendungen.
- Verwendung von nShield®-Hardware-Sicherheitsmodulen (HSM) von Entrust

Die Problemstellung: Aufgrund der steigenden Zahl an Geschäftsanwendungen müssen Unternehmen ihre PKI erweitern

Datenverletzungen werden immer ausgeklügelter. Daher setzen die Unternehmen beim Schutz und der Kontrolle des Zugriffs auf wichtige Anwendungen und sensible Daten auf ihre PKI. Die Zertifizierungsstelle (CA) stellt innerhalb der PKI elektronische Berechtigungsnachweise aus, um Online-Identitäten zu überprüfen und Zugriffskontrollen durchzusetzen. Damit die PKI die steigenden Anforderungen erfüllen kann, ist es wichtig, die Anzahl der verwendeten Zertifikate sowie die Wichtigkeit und den Wert der Anwendungen, die sie unterstützen, zu analysieren. Außerdem sollte untersucht werden, ob Anwendungen hinsichtlich der Einhaltung von staatlichen oder regulatorischen Vorschriften einer verstärkten Überprüfung unterliegen.



nShield HSM sichern die vom Red Hat Certificate System verwendeten Schlüssel.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Hochsicherer Schlüsselschutz für Red Hat Certificate System

Die Herausforderung: Bereitstellung eines Vertrauensankers für Identitäts- und Zugriffskontrollen

Der Schutz der Integrität und Sicherheit der CA, die einer PKI zugrunde liegt, ist von entscheidender Bedeutung, wenn es darum geht, Vertrauen in Unternehmensanwendungen aufzubauen und Daten verlässlich zu schützen. PKI müssen zunehmend an sich stetig verändernde Benutzerstrukturen wie die Nutzung von Mobilgeräten und Bring-you-own-Device (BYOD) angepasst werden.

Die Lösung: Red Hat und Entrust stellen gemeinsam robusten Schutz für digitale Identitäten bereit

Red Hat Certificate System übernimmt die Ausstellung, Verwaltung und Überprüfung der digitalen Identitäten, die zur festen Zuordnung von Personen, Geräten oder Dienste an die entsprechenden privaten Schüssel verwendet werden. Die Gültigkeit der jeweiligen ausgestellten Zertifikate hängt vom Schutz der CA ab, die diese Identitäten ausstellt. Wenn das Zertifikat auf einem Server mit einem Schlüssel ausgestellt wird, der lokal in einer Datei gespeichert ist, besteht die Gefahr, dass dieser Schlüssel dupliziert, modifiziert oder ersetzt wird. Heute werden Zertifizierungsstellen zumeist genutzt, um Zertifikate für die interne Verwendung in Unternehmen auszustellen. Diese Zertifikate werden in der Regel zur Authentifizierung (kabellos, mit Kabel oder über ein Virtual Private Network (VPN)) sowie für Secure-Socket-Layer/Transport-Layer-Security-Verbindungen (SSL/TKS-Verbindungen) verwendet. Da immer mehr Anwendungen die PKI nutzen, sind die Ansprüche an die Zertifizierungsstellen und der zusätzliche Sicherheitsbedarf von Vorrang.

nShield HSM von Entrust erhöhen das Sicherheitsniveau der PKI, die die privaten Root- und Signaturschlüssel schützt, und sichern die Ausstellung, Verwaltung und den Validierungsprozess. Dadurch können Unternehmen ihre Identitäts- und Zugangslösung verstärken. nShield HSM lassen sich über eine standardmäßige Cryptographic Application Programing Interface (CAPI) ganz einfach in das Red Hat Certificate System integrieren. Die Ausstellung und Validierung aller Zertifikate geschieht innerhalb der geschützten Grenzen des HSM. Private Root- und Signaturschlüssel werden unzugänglich oder in einem nicht lesbaren Format außerhalb des HSM aufbewahrt. Die nShield HSM stellen auch während des Backups, der Archivierung und Wiederherstellung sicher, dass private Schlüssel nicht manipuliert werden können und/oder in sonstiger Weise gefährdet sind.

Hochsicherer Schlüsselschutz für Red Hat Certificate System

Warum HSM von Entrust mit Red Hat Certificate System?

Das Erkennen von Datenschutzverletzungen sowie die Wiederherstellung und Notfallplanung sind wichtige Schritte zur Optimierung der Sicherheit einer PKI. Eine robuste, hochsichere PKI schützt sicherheitskritische Schlüssel vor Diebstahl und Missbrauch. Vergangene Probleme mit der Sicherheit von Zertifizierungsstellen haben dazu geführt, dass die Ausstellung von Zertifikaten heute mit der Prüfung und Genehmigung von Identitäten durch ein nShield HSM von Entrust verknüpft ist.

nShield HSM sind nach strengen Sicherheitsstandards einschließlich FIPS 140-2 Level 3 und Common Criteria EAL 4+ zertifiziert und sorgen für die:

- Speicherung der Schlüssel zur Ausstellung und Signatur von digitalen Zertifikaten in einer geschützten, manipulationssicheren Umgebung.
- Verwaltung des Administratorzugriffs mit Smartcard-basierten Richtlinien und Zwei-Faktor-Authentifizierung
- Einhaltung der regulatorischen Anforderungen für den öffentlichen Sektor, Finanzdienstleistungen und Unternehmen

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.

Red Hat

Red Hat ist der weltweit führende Anbieter von Open-Source-Lösungen für Unternehmen. Außer Red Hat Certificate Systems stellt er die Plattformen Red Hat Enterprise Linux, Red Hat OpenStack und Red Hat OpenShift sowie eine große Auswahl an Managementlösungen und Diensten bereit. Die nShield HSM sind gemäß dem Red Hat Certificate System zertifiziert. **www.redhat.com**

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