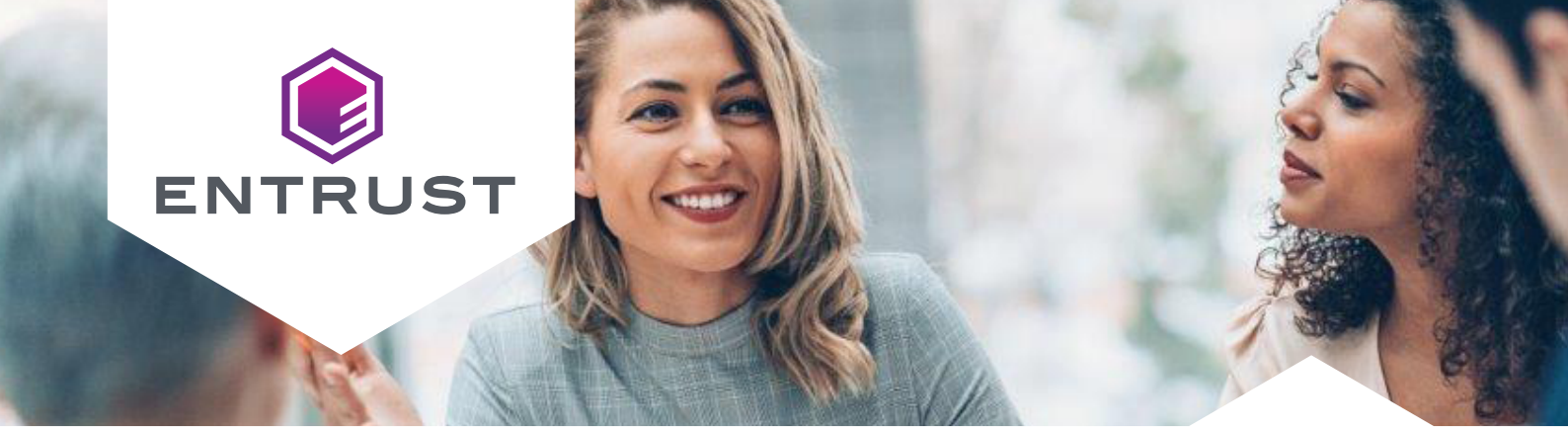


Microsoft und Entrust erhöhen das Vertrauen in das Internet der Dinge und optimieren die Sicherheit

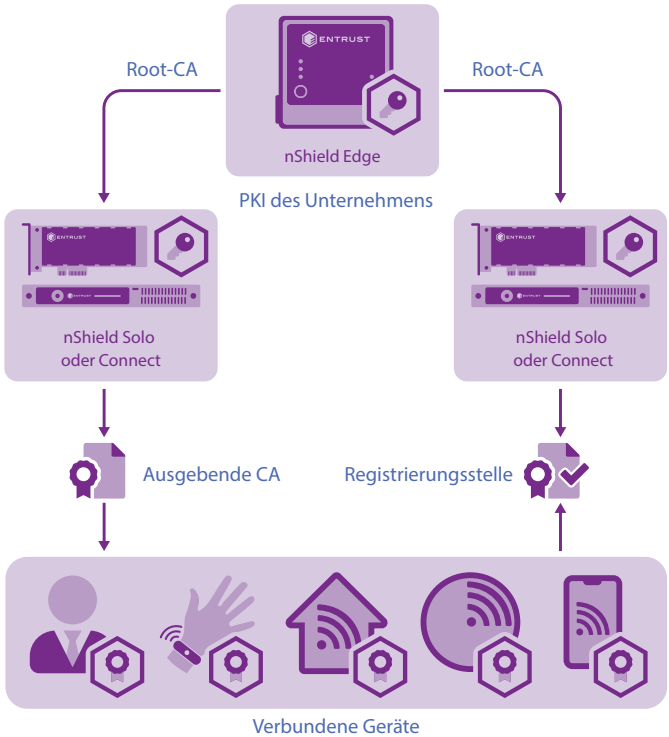
Dienste zur Geräteanmeldung und Hardware-Sicherheitsmodule ermöglichen die sichere Registrierung von IoT-Geräten

ECKPUNKTE

- Mehr Integrität für die Zertifikate von Netzwerkgeräten
- Nutzung bestehender PKI zur Unterstützung der Geräteregistrierung
- Sichere Speicherung und Verwaltung von Schlüsseln
- Gemäß FIPS 140-2 Level 3 validierter Schlüsselschutz
- Einfache Einhaltung von Datenschutzvorschriften

Die Problemstellung: eine steigende Zahl mit dem Internet verbundener Netzwerkgeräte, die digitale Zertifikate zur Identifizierung und Authentifizierung verwenden, muss auch die Registrierung von Zertifikaten unterstützen.

Je mehr Geräte und Unternehmensnetzwerke mit dem Internet verbunden sind, desto wichtiger ist es, diese zu identifizieren und authentifizieren. Nicht autorisierte Geräte können Vektoren für das Einschleusen von Malware in geschlossene Domains darstellen und ein signifikantes Risiko bergen. Public Key Infrastructure (PKI) dient dazu, Zugangsdaten zur Identifizierung und Authentifizierung von Geräten auszustellen und zu verwalten. Darüber hinaus ist ein vertrauenswürdiges Registrierungsverfahren erforderlich.



nShield HSM von Entrust schützen nicht nur die Root- und Ausgabe-CA von PKI, sondern auch die privaten Schlüssel, die verwendet werden, um Gerätezertifikate mit dem CA-Vertrauensanker zu verknüpfen und deren Integrität und Prüfung zu gewährleisten.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Microsoft und Entrust erhöhen das Vertrauen in das Internet der Dinge und optimieren die Sicherheit

Die Problemstellung: eine steigende Zahl verbundener Geräten soll mit vertrauenswürdigen domainbasierten Zugangsdaten sicher Zertifikate registrieren.

Die Ausstellung von Gerätezertifikaten ist nur der erste Schritt der Bereitstellung einer sicheren Netzwerkumgebung, in der sich eine steigende Zahl autorisierter Geräte mit einer geschützten Domain verbindet. Diese Zertifikate werden durch eine Zertifizierungsstelle (CA) registriert. Das dient der Prüfung und Kontrolle von Geräteverbindungen. Der Schutz und die Verwaltung kryptographischer Schlüssel, die den Registrierungsprozess unterstützen, sind unerlässlich, um Vertrauen in das gesamte System aufzubauen.

Die Lösung: Microsoft und Entrust ermöglichen gemeinsam die sichere Registrierung der Zertifikate verbundener Geräte

Der Network Device Enrollment Service (NDES) ist Teil der Active Directory Certificate Services (AD CS) von Microsoft. Mithilfe des Simple Certificate Enrollment Protocols (SCEP) definiert er die Kommunikation zwischen verbundenen Geräten und einer Registrierungsstelle für Zertifikate. Cloud-basierte und On-Premises-Lösungen wie Microsoft Intune und System Configuration Manager nutzen NDES zur Bereitstellung und Registrierung von Geräten. NDES ermöglicht die Registrierung und Validierung digitaler Geräteidentitäten, die mit Windows-Servern verbunden sind, indem er diese mit einem entsprechenden privaten Schlüssel verknüpft. Die Dienste nutzen eine CA als Vertrauensanker und machen damit die Registrierung von Zertifikaten sowie die Überprüfung ihrer Authentizität und Integrität möglich.

Wenn das Zertifikat auf einem Server mit einem Schlüssel ausgestellt wird, der lokal in einer Datei gespeichert ist, besteht die Gefahr von Angriffen, wodurch dieser Schlüssel dupliziert, modifiziert oder ersetzt werden kann. Die nShield-Hardware-Sicherheitsmodule (HSM) von Entrust erhöhen die Sicherheit des Verfahrens zur Registrierung der Zertifikate, indem sie den privaten NDES-Schlüssel schützen. Die nShield® HSM von Entrust können mithilfe der standardmäßigen kryptographischen Anwendungsprogrammierschnittstelle (CAPI) von Microsoft in Microsoft NDES integriert werden.

Warum HSM von Entrust mit Microsoft NDES?

Das schnelle Wachstum des Internet of Things (IoT) hat zur Folge, dass immer mehr verbundene Geräte bereitgestellt werden. PKI soll nicht nur den privaten Root-CA-Schlüssel, der die Sicherheit der ausgestellten Zertifikate in der gesamten Domain untermauert, sondern auch die Registrierung dieser steigenden Zahl an Zertifikate schützen. Unternehmen, die in ihren PKIs keine HSM zum Schutz ihrer privaten Schlüssel verwenden und keine Maßnahmen zur Registrierung und Überprüfung von Zertifikaten ergreifen, sind anfällig für Störungen mit möglicherweise schwerwiegenden Folgen. HSM bieten eine robuste Umgebung, die sicherheitskritische Schlüssel vor Verlust und Missbrauch schützt. Mit Failover-Unterstützung ermöglichen sie, die Schlüssel über ihren gesamten Lebenszyklus zu verwalten, wobei mehrere HSM für eine hohe Verfügbarkeit sorgen. 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 sowie der Registrierung und Validierung von Zertifikaten verknüpft ist.

Microsoft und Entrust erhöhen das Vertrauen in das Internet der Dinge und optimieren die Sicherheit

nShield HSM von Entrust sind nach strengen Sicherheitsstandards einschließlich FIPS 140-2 Level 3 zertifiziert und:

- speichern Root-CA und die Registrierungsschlüssel in einer geschützten 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

HSM von Entrust

Die nShield HSM von Entrust unterstützen AD CS seit der Veröffentlichung von Windows Server 2003 und wurden seitdem weltweit einer großen Zahl von Kunden bereitgestellt. Die Unterstützung von NDES ist eine Erweiterung dieses Dienstes. nShield HSM vereinfachen die Verwaltung von Zugangsdaten für eine Vielzahl von Anwendungen und PKIs. Sie können in virtuellen Umgebungen einschließlich Hyper-V eingesetzt werden. Die nShield HSM von Entrust unterstützen Unternehmen dabei, Anforderungen an Prüfungen und die Einhaltung von Vorgaben wie den Payment Industry Security Standard (PCI DSS) einzuhalten und sind in den folgenden Varianten erhältlich.

- nShield Edge: portables HSM mit USB-Anschluss für Offline-Root-CAs
- nShield Solo XC: integriertes PCI-Express-Hochleistungs-HSM für Server
- nShield Connect XC: netzwerkgebundenes äußerst leistungsstarkes HSM für Rechenzentren

Microsoft

Microsoft hat die Art und Weise, in der Unternehmensressourcen geteilt und Identitäten und Zugriffskontrolle verwaltet werden, einschneidend verändert. Systeme auf der Grundlage von Microsoft AD CS und NDES bieten individuelle Dienste für das Erstellen und die Verwaltung öffentlicher Schlüsselzertifikate. So entstehen vertrauenswürdige Geschäftsumgebungen zwischen Menschen und Geräten. Microsoft NDES:

- stellt Gerätezertifikate über Registrierungsstellen bereit und registriert diese
- sichert die Registrierung domain-basierter Zugangsdaten
- ermöglicht es, Zertifikate zu überprüfen und zu widerrufen

www.microsoft.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