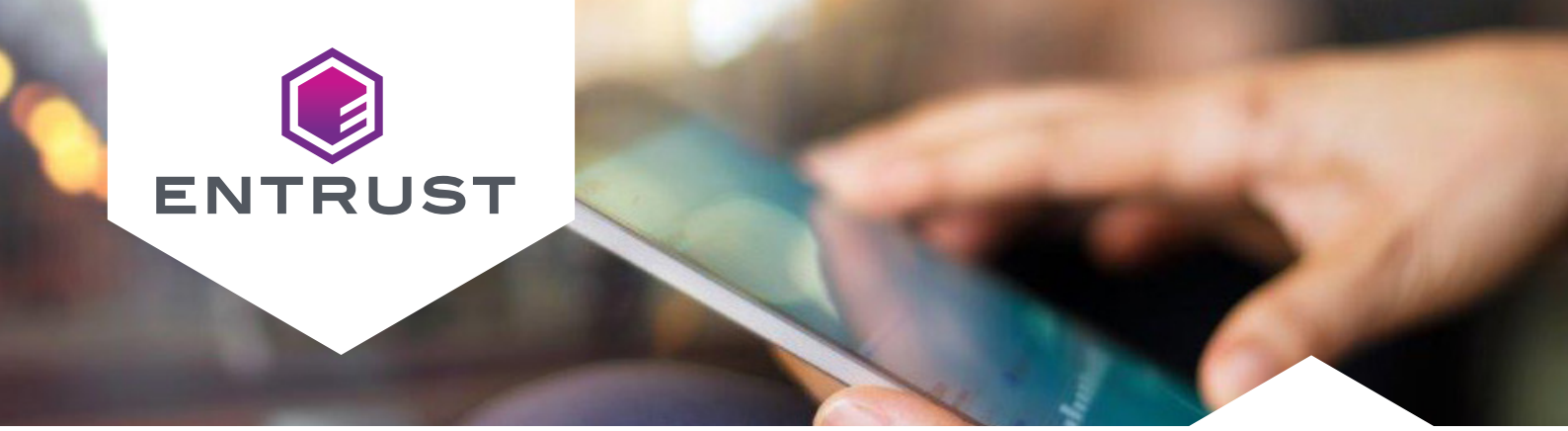


nShield Web-Services-Optionspaket

Cloud-freundliche REST-ähnliche Schnittstelle zu hochsicheren Hardware-Sicherheitsmodulen

HIGHLIGHTS

- Zugriff auf eine äußerst sichere Datenschutzlösung in der Cloud, im Rechenzentrum oder in On-Premises-Anwendungen
- Optimierte und einfache Verbindung zu kryptographischen Diensten des nShield-Hardware-Sicherheitsmoduls
- Schnelle und skalierbare dynamische Anwendungsbereitstellung
- Unterstützung unterschiedlicher Betriebssysteme und Architekturen

Das nShield Web-Services-Optionspaket (WSOP) bietet eine REST[1]-ähnliche API zwischen Anwendungen, die kryptographische Schlüssel- und Datenschutzdienste benötigen, und FIPS-zertifizierten nShield Hardware-Sicherheitsmodulen (HSM). nShield HSM führen eine Vielzahl kryptographischer Funktionen einschließlich Verschlüsselung, Entschlüsselung, Signierung, Verifizierung und Schlüsselerstellung aus. Diese Kernfunktionen stehen Anwendungen jetzt über eine einfache Webservice-Schnittstelle unter Verwendung des universellen HTTPS-Protokolls zur Verfügung.

WICHTIGE FUNKTIONEN UND VORTEILE

- **Effizienter Zugriff auf externe kryptographische Dienste aus der Cloud, aus dem Rechenzentrum oder aus lokalen Anwendungen:** Anwendungen, die sich an einem beliebigen Ort befinden – sei es in der Cloud, in entfernten Rechenzentren oder lokal – können mittels https-basierter Webservice-Aufrufe über die REST-ähnliche API auf nShield-Dienste zugreifen, was mehr Flexibilität in die heutigen vielfältigen Computerumgebungen bringt.
- **Optimierter Entwicklungsprozess:** Die effiziente und moderne Webservice-Schnittstelle verbessert die Geschwindigkeit, mit der Anwendungen für den Zugriff auf nShield HSM-Kryptodienste entwickelt werden können.
- **Keine kundenseitige Integration erforderlich:** Typischerweise erfordert die Integration von Anwendungen mit nShield-HSM die Bindung an lokale Host-Bibliotheken und die Bereitstellung lokaler Dienste. Entwickler profitieren von der REST-ähnlichen API für Webservices, da diese die Bereitstellung vereinfacht.

nShield Web-Services-Optionspaket

- **Unterstützung unterschiedlicher Betriebssysteme und Architekturen:** Die REST-ähnliche Webservice-Schnittstelle ist unabhängig von der Anwendungsinfrastruktur des Kunden und erfordert keine lokale betriebssystemspezifische Software, was die Integration insbesondere in kundenspezifischen Umgebungen erleichtert.
- **Dynamisch skalierbar:** Für neue oder zusätzliche Anwendungs-Workloads sind keine weitere HSM-Konfiguration, Installation von Support-Software oder Kundenlizenzen erforderlich. Passen Sie Ihre Kapazität einfach an die Nachfrage an – einschließlich WSOP-Knoten für den Einsatz in einer Container-Architektur.
- **Unterstützung der Lastverteilung durch dedizierte seriengefertigte Geräte:** Das WSOP ermöglicht die Verwaltung der HSM-Workloads mithilfe kommerzieller, seriengefertigter Load Balancer, die die HSM-Bereitstellung/Konfiguration vereinfachen und die beste Nutzung eines Pools von HSM gewährleisten.

Bereitstellung des nShield Web-Services-Optionspaket

Voraussetzungen:

- Security World Software v12.6x oder höher
- nShield Solo, Connect HSM oder nShield-as-a-Service-Abonnement

Um die REST-ähnliche API zu verwenden, wird das nShield WSOP auf einem nShield-Client-Server installiert, wodurch der Dienst aktiviert und für direkte und sofortige Verbindungen von Anwendungen aus verfügbar gemacht wird.

Das WSOP ist standardmäßig mit einem Satz temporärer, kurzfristiger TLS-Zertifikate zu Testzwecken konfiguriert. Die Konfiguration sollte mit entsprechenden Zertifikaten für laufende Tests oder den Produktionseinsatz aktualisiert werden.

Für nShield Connect-HSM: Eine übliche Client-Lizenz ist nur für den Client-Server erforderlich, auf dem der Webdienst ausgeführt wird. Für die Verbindung von Anwendungen sind keine Client-Lizenzen erforderlich.

Anmerkung 1: REST (REpresentational State Transfer) ist eine auf Webstandards basierende Architektur, welche das universelle HTTP-Protokoll zur Datenkommunikation verwendet. HTTP wird als ein zustandsloses Protokoll betrachtet, da jeder Befehl unabhängig ausgeführt wird, ohne Kenntnis der vorhergehenden Befehle. REST ist ressourcenbasiert, wobei jede Komponente als eine Ressource betrachtet wird, auf die über eine gemeinsame Schnittstelle mittels HTTP-Aufrufen zugegriffen wird.

Zu den REST-Eigenschaften von WSOP gehören:

- gut definierte URI, die „Ressourcen" eindeutig identifizieren, z. B. Schlüssel/Zeichen/Verifizieren usw.
- HTTP-Methoden, um Aktionen auf dieser Ressource durchzuführen, z. B. GET für Leseoperationen wie das Auflisten von Schlüsseln, POST für Schreiboperationen wie das Erstellen von Schlüsseln, DELETE für Löschoperationen wie das Löschen von Schlüsseln.

nShield Web-Services-Optionspaket

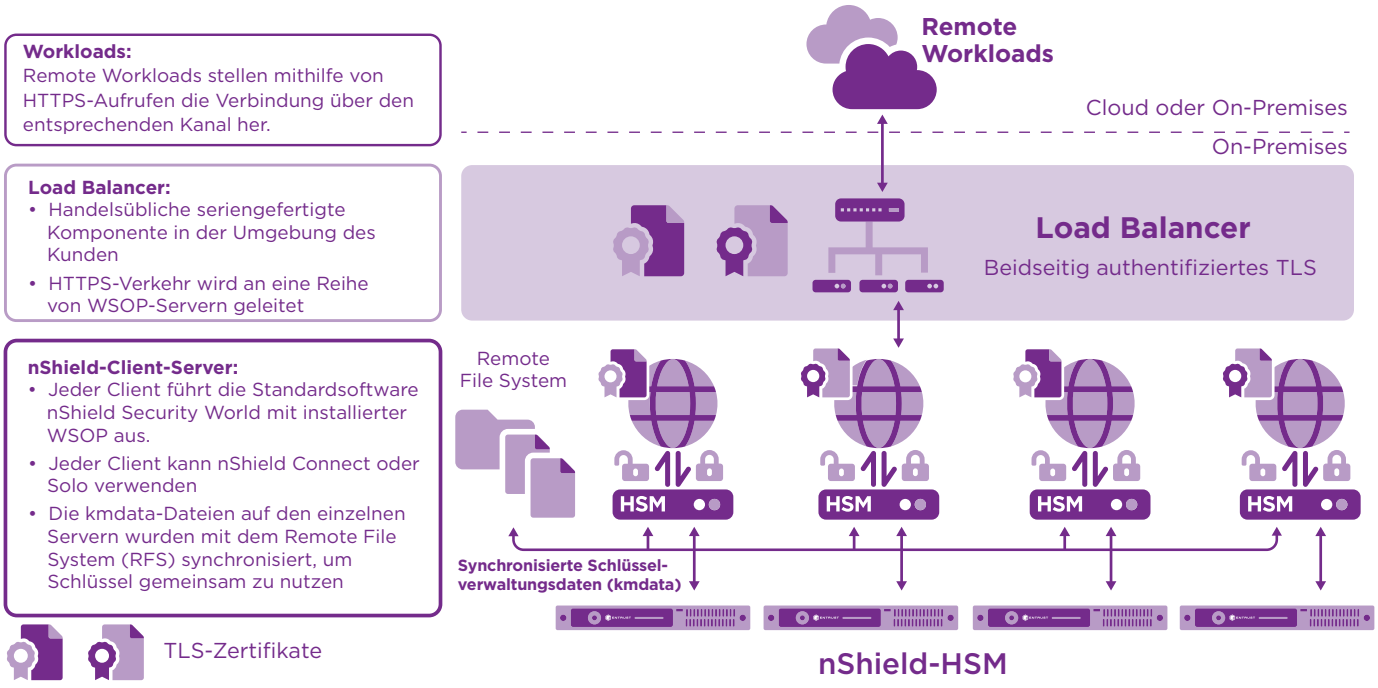
TECHNISCHE DATEN

nShield-Kompatibilität

Das nShield WSOP ist mit allen Modellen der nShield-Solo- und Connect-HSM kompatibel. Das WSOP muss auf einem Host installiert sein, auf dem eine unterstützte Version des Linux-Betriebssystems sowie die nShield Security World Software läuft. Es unterstützt durch Operator Card Set und Softcard geschützte Schlüssel. Das WSOP ist auch mit dem nShield Container Option Pack kompatibel, so dass es in einer containerisierten Umgebung bereitgestellt werden kann.

API-Kompatibilität

nShield-HSM unterstützen Anwendungen, die die Webservice-Schnittstelle, sowie Anwendungen, die andere unterstützte Schnittstellen (PKCS # 11, Java, CNG usw.) verwenden.



Typische WSOP-Bereitstellung

Weitere Informationen

Mehr Informationen zu den nShield HSM 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 HSM

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