Schlüsselspeicher mit hoher Skalierbarkeit

Millionen von Schlüsseln gleichzeitig mit hoher Leistung handhaben

ECKPUNKTE

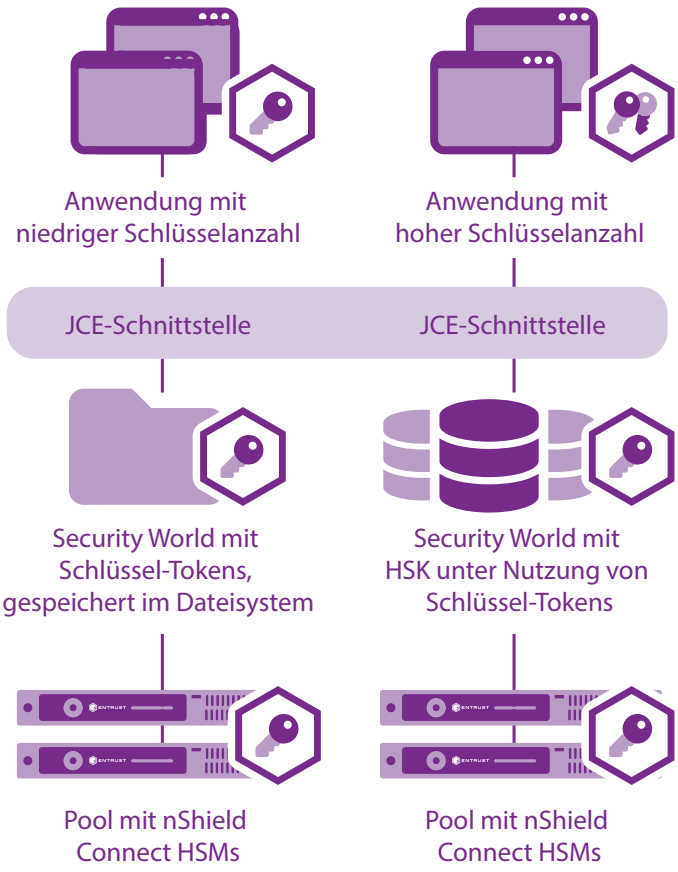
- Eine leistungsstarke, skalierbare Lösung für bestimmte Anwendungsfälle von Entrust nShield® HSMs
- Unterstützt eine sehr hohe Anzahl an gleichzeitig aktiven kryptographischen Schlüsseln
- Verhindert Engpässe im Betriebssystem

In manchen Fällen müssen Hardware-Sicherheitsmodule (HSM) eine sehr hohe Anzahl an kryptographischen Schlüsseln gleichzeitig handhaben. Das kann zu Engpässen im Dateisystem des Rechners führen, der mit den HSMs verbunden ist. Ein Schlüsselspeicher mit hoher Skalierbarkeit (high-scalability keystore, HSK) unterstützt diese großen Mengen an Schlüsseln mit hoher Leistung.

Wichtige Funktionen

Die HSK-Lösung bietet die folgenden Funktionen:

- Skalierbar zu Millionen von RSA-Schlüsseln
- Leistung bleibt während des Anstiegs der Schlüsselzahl praktisch unverändert
- Unterstützt die Erstellung von RSA-Schlüsseln, die Erstellung von Certificate Signing Requests (CSR), die Erstellung und Verifizierung digitaler Signaturen sowie Datenverschlüsselung und -entschlüsselung.
- Automatische Synchronisation zwischen mehreren abrufenden Rechnern
- Personalisierbare, erweiterbare Lösung, die zu Ihren Bedürfnissen passt



MEHR INFORMATIONEN AUF ENTRUST.COM/HSM

nShield Edge HSM

Funktionsweise

Entrust nShield HSMs bieten einen leistungsstarken Transaktionsdurchsatz, der Tausende von Transaktionen pro Sekunde unterstützt. (Die Leistung hängt vom HSM-Modell und dem spezifischen Verschlüsselungsbetrieb ab. Siehe Datenblatt für spezifische nShield-Modelle für die neuesten Daten zur HSM-Leistung.)

Die flexible und sichere Security-World-Architektur von Entrust speichert kryptographische Schlüssel fernab vom HSM als „Tokens“. Die Schlüssel innerhalb dieser „Tokens“ unterstehen mittels Verschlüsselung, Nutzungsbeschränkungen, Zugriffskontrollen und Authentifizierungssicherheit dem starken Schutz der HSM-Master-Schlüssel. So werden eine sehr starke Sicherheit mit verschiedenen Vorteilen kombiniert: Skalierbarkeit, Load-Balancing, Failover, einfache Erweiterung oder Reduzierung der Anzahl an HSMs in einem Pool, Austausch von HSMs im Pool sowie einfaches Back-up von Schlüsseltokens ohne zusätzlich erforderliche Back-up-Geräte.

Die standardmäßige Security-World-Architektur speichert diese „Tokens“ in den Dateisystemen der abrufenden Rechner (mit unterstützter Synchronisation) mithilfe einer einzelnen Datei pro Token ab. Dieser Ansatz eignet sich für die meisten Anwendungsfälle, die üblicherweise eine begrenzte Anzahl an aktiven Schlüsseln pro Kundenrechner aufweisen.

In gewissen Anwendungsfällen kann die Leistung der nShield HSMs aufgrund von Latenzen im Dateisystem des Betriebssystems des abrufenden Rechners eingeschränkt sein. HSK bietet eine hohe Leistung, wenn eine enorme Zahl an Schlüsseln vorhanden ist, indem eine Datenbank anstelle eines Dateisystems verwendet wird, um Schlüsseltokens im Kundenrechner zu speichern.

Das Team von Entrust Professional Services (PS) hilft Ihnen dabei zu bestimmen, ob ein HSK Ihren Bedürfnissen entspricht. PS-Berater unterstützen Sie außerdem mit fachmännischem Entwicklungs-Support für die Integration des HSK in Ihre Umgebung. Dazu gehört, dass das HSK an Ihre spezifischen Anforderungen angepasst wird.

Anwendungsbeispiele

- E-Mail-Sicherheit in Unternehmen für eine Vielzahl an Benutzern
- Dokumentunterzeichnung in Unternehmen
- Internet of Things (IoT) mit einer Vielzahl an verbundenen Geräten
- Mobile Apps mit einer Vielzahl an Endnutzern
- eWallet-Systeme für Kryptowährungswechsel

Technische Details

- Bibliothek der Java Cryptography Extension (JCE) mittels nShield HSMs
- RESTful JSON-Web-Services-Option
- Speichert nShield HSM-Schlüsseltokens in einer Datenbank anstelle eines Dateisystems
- Einsatz möglich mit gängiger relationaler Datenbanksoftware wie MSSQL, Oracle und Derby (zusätzliche Datenbanken folgen)
- Einsatz möglich mit einzelnem HSM oder mehreren HSMs in einem Load-Balance-Pool

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.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com