Nitrokey HSM

Sicherer Schlüsselspeicher mit professioneller Schlüsselverwaltung.

Was bisher nur teure und proprietäre Hardware-Sicherheitsmodule (HSM) leisteten, kommt nun als Open Hardware zu einem unschlagbar günstigen Preis aus Deutschland. Nitrokey HSM schützt Ihre kryptografischen Schlüssel zuverlässig – mit verschlüsselten Backups, Vier-Augen-Zugriffsschutz und vielen weiteren Sicherheitsfunktionen. Mit USB-Schnittstelle ist Nitrokey HSM die ideale Lösung für Zertifikatsinfrastrukturen jeder Art und Größe.

Nitrokey
secure your digital life

Anwendungsfälle

PKI und CA betreiben

Nitrokey HSM bietet Ihnen sichere Schlüsselgenerierung, -speicherung und -verwaltung – für Public Key Infrastrukturen (PKI), Certificate Authorities (CA) und sonstige zentrale Signaturschlüssel. Technische Sicherheitsfunktionen ersetzen teure organisatorische Schutzmaßnahmen, wie z. B. die Schlüsselablage in mehreren Bankschließfächern, und schützen Ihre Schlüssel auch bei großen und wechselnden Teams.

Compliance-Anforderungen erfüllen (z. B. PCI DSS)

Gemäß PCI DSS müssen Schlüssel, mit denen Kreditkartendaten ver-/entschlüsselt werden, jederzeit sicher gespeichert sein. Als ein Baustein hilft Ihnen Nitrokey HSM, die PCI-DSS-Anforderungen zu erfüllen und Ihre PCI-DSS-Zertifizierung zu erreichen.

Internet of Things (IoT) und eigene Produkte schützen

Schützen Sie Ihre eigenen Hardware-Produkte durch Integration des Nitrokeys. Ideal zur Fernwartung und zur Gewährleistung der Produktechtheit.

Server sicher mit SSH administrieren

Haben Sie Ihren SSH-Schlüssel immer sicher im Nitrokey dabei. Ihr Schlüssel ist PIN-geschützt und kann nicht aus dem Nitrokey exportiert/gestohlen werden.

E-Mails verschlüsseln

Für die E-Mail-Verschlüsselung mittels S/MIME speichern Sie Ihre privaten Schlüssel sicher im Nitrokey HSM. So sind Ihre Schlüssel gegen Verlust, Diebstahl und Computerviren geschützt.

FUNKTIONEN

Vier-Augen-Zugriffsschutz / *M*-von-*N*-Verfahren

Um Zugriff auf die kryptografischen Schlüssel zu erhalten, müssen *M* von *N* Schlüsselverwaltern zustimmen. Eine einzelne Person alleine erhält keinen Zugriff. Falls einzelne Schlüsselverwalter ausfallen, ist der Schlüsselzugriff weiterhin möglich, solange mindestens *M* Schlüsselverwalter verfügbar sind. Somit bleiben Ihre Schlüssel auch bei großen und wechselnden Teams immer geschützt.
Schlüsselverwalter können sich entweder mit einem eigenen Nitrokey HSM (für *M*-von-*N*-Zugriffsschutz erforderlich) oder mittels Passwort authentisieren. Fernzugriff ist möglich, so dass die Schlüsselverwalter nicht physisch am selben Ort anwesend sein müssen.

Eingebaute PKI-Funktion

Mit der eingebauten PKI-Funktion lassen sich im Nitrokey HSM generierte Schlüssel signieren. So kann eine externe Stelle (z. B. CA) die Authentizität, Integrität und Herkunft der Schlüssel überprüfen. Das vorinstallierte Wurzelzertifikat von unserem Partner CardContact ermöglicht es, individuelle und gültige Gerätezertifikate je Nitrokey HSM zu erstellen. Auf Wunsch kann ein eigenes Wurzelzertifikat verwendet werden. Eine weltweit einmalige Geräte-ID erlaubt die kryptografische Überprüfung der Nitrokey HSM.

Verschlüsselte Backups

Nitrokey HSM unterstützt Schlüsselbackups zum Schutz gegen Datenverlust. Hierbei sind die Backups mit dem Device Key Encryption Key (DKEK) verschlüsselt. Da der DKEK ausschließlich in andere Nitrokey HSM eingebracht werden kann, ist sichergestellt, dass Backups jederzeit verschlüsselt und nicht außerhalb eines Nitrokey HSM entschlüsselbar sind.

Schlüsselbeschränkung

Für jeden Schlüssel lässt sich dessen Nutzung einschränken (z. B. anhand Algorithmus, Verwendungszweck, Backuperlaubnis). Diese Beschränkungen legen Sie bei der Schlüsselgenerierung fest und gelten für den gesamten Lebenszyklus des Schlüssels. Somit sind die Einhaltung zulässiger Algorithmen und des korrekten kryptografischen Verwendungszwecks sichergestellt.

Schlüsselzähler

Ein Schlüsselzähler ermöglicht, die Schlüsselnutzung nachzuvollziehen und einzuschränken. Einmal im Rahmen der Schlüsselgenerierung definiert, zählt der Schlüsselzähler mit jeder Schlüsselnutzung rückwärts. Sobald die maximale Anzahl an Schlüsselnutzungen erreicht ist, wird der Schlüssel gesperrt.

Schlüsselimport

Sie können bestehende Schlüssel in den Nitrokey HSM importieren; z. B. bei einer CA-Schlüsselmigration, Schlüssel aus einem PKCS#12-Container in ein passendes, importierbares Format umwandeln. Unser Rat: Generieren Sie Ihre Schlüssel immer im Nitrokey HSM, so dass diese über ihren gesamten Lebenszyklus hinweg geschützt bleiben.

Sicherer Kanal

Sie können lokal oder aus der Ferne (remote) einen verschlüsselten Kommunikationskanal zum Nitrokey HSM verwenden (ähnlich wie SSL/TLS). So sind der Datenaustausch (z. B. PIN, signierte Daten) und die Integrität der Gerätebefehle abgesichert.

Transport-PIN

Eine frei wählbare Transport-PIN erlaubt die Absicherung des Gerätetransports zum Nutzer. Mit Hilfe der Transport-PIN kann der Nutzer sicherstellen, dass der Nitrokey HSM unterwegs nicht manipuliert wurde. Der Nutzer muss vor dem erstmaligen Zugriff die Transport-PIN in eine eigene PIN ändern.

PIN-Verwaltung

Nitrokey HSM bietet einen Initialisierungscode (SO-PIN) zum Schutz der Geräteinitialisierung und eine Nutzer-PIN zum Zugriffsschutz. Zur Verhinderung von Brute-Force-Angriffen lässt sich die maximale Anzahl von PIN-Eingabeversuchen konfigurieren.

Starke Authentisierung

Zur Authentisierung können Sie PIN oder Schlüssel verwenden. Für letzteres registrieren Sie während der Ersteinrichtung eines Nitrokey HSM einen Schlüssel eines anderen Nitrokey HSM. Bei der Authentisierung mittels Nitrokey HSM kommt ein Challenge-Response-Verfahren zum Einsatz.

Unterstützte Systeme und Schnittstellen

- X.509, S/MIME
- PKCS#11 (Public Key Cryptography Standards)
- Cryptographic Service Provider (CSP) Minidriver für Windows
- C Application Programming Interface (API)
- Java Cryptography Extension (JCE) Provider
- OpenSC und Open Smart Card Development Platform (OpenSCDP)
- CA-Verwaltungssoftware: XCA, EJBCA
- GnuPG - S/MIME-Version
- Windows, macOS, Linux, BSD

Technische Details

- Kryptografiealgorithmen: RSA, ECC
- Schlüssellängen: RSA 1024, 1536, 2048 Bit; ECC 192, 224, 256, 320 Bit
- Padding/Varianten: RSAES-OAEP, RSAES-PKCS1-v1_5, RSASSA-PSS, RSASSA-PKCS1-v1_5, ECDH, ECDH mit HMAC KDF, ECDSA
- Elliptische Kurven: secp192r1/prime192v1, secp256r1/prime256v1, brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, secp192k1, secp256k1 (Bitcoin)
- Hash-Algorithmen: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, internes und externes Hashing unterstützt
- Speicherkapazität: max. 31 x ECC-256 Schlüssel, max. 20 x RSA-2048 Schlüssel, 124 x Datenobjekte (DF, EF) je 256 Byte mit insg. 32 KB
- Signaturgeschwindigkeit ohne Hashing: ECDSA-256: 360 Signaturen/Min., RSA-2048: 100 Signaturen/Min.
- Schlüsselerzeugung: ECC-256: 10 Schlüssel/Min., RSA-2048: 2 Schlüssel/Min.
- Card Verifiable Certificates (CVC) entsprechend BSI TR-03110 (Extended Access Control)
- Physikalischer Zufallszahlengenerator (TRNG): Güte DRG.3 nach AIS-31
- Verschlüsselte Backups: AES-256
- Sicherer Kanal: AES-128, 3DES-112
- Lebensdauer (MTBF, MTTF): > 500.000 PIN-Eingaben
- Speicherdauer: > 25 Jahre
- Aktivitätsanzeige: einfarbige LED
- Hardware-Schnittstelle: USB 1.1, Typ A
- Größe: 48 x 19 x 7 mm
- Gewicht: 6 g
- Konformität: FCC, CE, RoHS, WEEE, OSHwA

NITROKEY IST BESSER

Hohe Sicherheit

Ihre kryptografischen Schlüssel werden den gesamten Lebenszyklus über in einem oder mehreren Nitrokey HSM sicher gespeichert. Beginnend bei der Schlüsselgenerierung, über den verschlüsselten Export und Import, bis hin zur Nutzung: Nitrokey HSM schützt Ihre Schlüssel gegen externe Angreifer und Innentäter. Schutz gegen Brute-Force-Angriffe verhindert das Erraten der PIN, indem das Gerät nach 15 Fehlversuchen gesperrt wird. Der verwendete Sicherheitschip und das Betriebssystem sind nach Common Criteria EAL 5+ zertifiziert.

Skalierbare Geschwindigkeit

Ein einziger Nitrokey HSM erfüllt bereits Geschwindigkeitsanforderungen von Offline- und Inhouse-CAs (siehe Abschnitt „Technische Details"). Sie können die Geschwindigkeit weiter erhöhen, indem Sie beliebig viele Nitrokey HSM verwenden/skalieren. Unser PKCS#11-Treiber unterstützt die Skalierung bei weiterhin einfacher Nutzung des Clusters.

Sicherheit erfordert Open Source

Sowohl Hardware als auch Firmware, Tools und Bibliotheken sind Open Source und Freie Software und ermöglichen unabhängige Sicherheitsüberprüfungen. Flexibel anpassbar, keine Herstellerabhängigkeit, keine Schein-Sicherheit durch Verschleierung, keine versteckten Sicherheitslücken.[1]

[1] Nitrokey HSM basiert auf SmartCard-HSM und beinhaltet daher proprietäre Komponenten anderer Hersteller.

Einfache Integration

Nitrokey verwendet offene Schnittstellen und Open Source Tools, um die einfache Integration in Ihre Systeme zu ermöglichen. Auf Wunsch entwickeln wir eine angepasste Lösung für Sie. Einfaches Anschließen per USB erspart kompliziertes Einbauen.

Besser als Software

Die Nitrokey-Hardware ist betriebssystemunabhängig und schützt Ihre Schlüssel zuverlässig gegen Diebstahl, Verlust, Benutzerfehler und Computerviren.

Besser als andere Hardware

Gegenüber Chipkarten erspart Nitrokey zusätzliche Kabel und Adapter. Ein vollwertiger USB-Stecker garantiert den einfachen und störungsfreien Anschluss an jedem marktüblichen Computer und Server.

Günstiger Preis

Zu einem Bruchteil des Preises herkömmlicher HSM bietet Nitrokey HSM hohe Sicherheit, hohe Qualität und professionellen Leistungsumfang. Ideal für Zertifikatsinfrastrukturen jeder Art und Größe.

Made in Berlin

Nitrokey wird in Berlin bzw. Deutschland entwickelt und produziert. Zugunsten höherer Qualität und Sicherheit verzichten wir auf eine billige Herstellung im Ausland.

www.nitrokey.com

Stand: 11/2018

Unsere Kunden