Datenblatt

Nitrokey HSM 2

Artikel-Nr.:	NK-HSM
Hersteller:	Nitrokey
EAN:	4322345307207
Herkunftsland:	Deutschland
Zolltarifnummer:	84718000
Gewicht:	0.009 kg

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.

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 and Open Smart Card Development Platform (OpenSCDP)
- CA-Verwaltungssoftware: XCA, EJBCA
- GnuPG - S/MIME-Version
- Windows, macOS, Linux, BSD

Technische Details

- Kryptografiealgorithmen: RSA, ECC, AES
- Schlüssellängen: RSA 1024-4096 Bit, ECC 192-521 Bit, AES 128-256 Bit
- Padding/Varianten: RSAES-OAEP, RSAES-PKCS1-v1_5, RSASSA-PSS, RSASSA-PKCS1-v1_5, ECDH, ECDH mit HMAC KDF, ECDSA
- Elliptische Kurven: SECG / NIST P-192, P-256, P-384, P-521 (secp192r1/prime192v1, secp256r1/prime256v1, secp521r1/prime521v1); Bitcoin Koblitz-Kurve: secp192k1, secp256k1, secp521k1; RFC 5639: brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r
- Hash-Algorithmen: SHA-1, SHA-256, SHA-384, SHA-512, internes und externes Hashing unterstützt
- Speicherkapazität: 76 KB EEPROM insgesamt, max. 150 x ECC-521 Schlüssel, max. 300 x ECC/AES-256 Schlüssel, max. 19 x RSA-4096 Schlüssel, max. 38 x RSA-2048 Schlüssel
- Geschwindigkeit (ohne Hashing): RSA-1024: 90 ms, RSA-1536: 150 ms, RSA-2048: 250 ms, RSA-3074: 1900 ms, RSA-4096: 4100 ms, ECDSA-256: 80 ms, ECDH-256: 90ms, ECDSA-512: 190 ms, ECDH-512: 290 ms
- Geschwindigkeit Schlüsselerzeugung: RSA-2048: 20 Sek., RSA-4096: 120 Sek., ECC-256: 6 Sek., ECC-512: 8 Sek.
- Card Verifiable Certificates (CVC) entsprechend BSI TR-03110 (Extended Access Control)
- Zufallszahlengenerator (RNG): Güte DRG.3 nach AIS-20
- 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
- Maximale Stromaufnahme: 50 mA
- Maximale Leistungsaufnahme: 250 mW
- Größe: 48 x 19 x 7 mm
- Gewicht: 6 g

Weitere Bilder: