Nitrokey HSM 2

Secure key storage with professional key management.

What was previously only provided by expensive and proprietary hardware security modules (HSM) is now available as open hardware at an unbeatably low price from Germany. Nitrokey HSM reliably protects your cryptographic keys with encrypted backups, two-man rule as access protection and many other security features. With a USB interface, Nitrokey HSM is the ideal solution for certificate infrastructures of any type and size.

Nitrokey
secure your digital life

Applications

Operating PKI and CA

Nitrokey HSM provides secure key generation, storage and management for public key infrastructures (PKI), certificate authorities (CA) and other central signing keys. Technical security features replace expensive organizational protection measures such as storing keys in safe deposit boxes, and even protect keys for large and changing teams.

Fulfilling Compliance Requirements (e.g. PCI DSS)

According to PCI DSS, keys that encrypt or decrypt credit card data must be securely stored at all times. Nitrokey HSM is a fundamental component that helps you to meet PCI DSS requirements and to achieve your PCI DSS certification.

Internet of Things (IoT) and Protecting Your own Products

Protect your own hardware products using Nitrokey integration. Ideal for remote maintenance and for ensuring product authenticity.

Securely Administrating Servers With SSH

Securely store your SSH keys in the Nitrokey at all times. Your key is PIN-protected and cannot be exported or stolen from the Nitrokey.

Encrypting Emails

Your private key can be stored securely in the Nitrokey HSM for email encryption by means of S/MIME. Your keys are thus protected against loss, theft and malware.

FEATURES

Two-Man Rule as Access Protection / *M*-of-*N* Threshold Scheme

In order to gain access to the cryptographic keys, *M* of *N* key administrators must approve. A single person alone cannot obtain access. If an individual key administrator is unavailable, key access is still possible, provided at least *M* key administrators are available. This means that your keys are always protected, even in large and changing teams.
Key administrators can either authenticate themselves using their own Nitrokey HSM (required for *M*-of-*N* access protection) or by means of a password. Remote access is possible, so key administrators do not have to be physically present in the same location.

Built-in PKI Feature

The built-in PKI feature can be used to sign keys which were generated in the Nitrokey. An external entity (e.g. CA) can check the authenticity, integrity and origin of the keys. The preinstalled root certificate from our partner CardContact makes it possible to create individual and valid device certificates for each Nitrokey HSM. On request, an own root certificate can be used. A unique device ID allows cryptographic verification of the Nitrokey HSM.

Encrypted Backups

Nitrokey HSM supports key backup to protect against data loss. The backups are encrypted with the device key encryption key (DKEK). Since the DKEK can only be imported to another Nitrokey HSM, backups are always encrypted and cannot be decrypted outside of a Nitrokey HSM.

Key Restriction

Each key's use can be restricted (e.g. by algorithm, purpose, backup permissions). These restrictions are determined at the time of key generation and are valid for the entire life cycle of the key. This ensures compliance with allowed algorithms and with the correct cryptographic purpose.

Key Counter

A key counter allows you to count and limit the use of keys. Once defined during key generation, the key counter counts down with each key usage. As soon as the maximum number of key uses is reached, the key is locked.

Key Import

You can import existing keys onto the Nitrokey HSM: for example, for a CA key migration by converting keys from a PKCS#12 container to a suitable, importable format. Our advice: Always generate your keys in the Nitrokey HSM so that they remain protected during their entire life cycle.

Secure Channel

You can use an encrypted communication channel with the Nitrokey HSM locally or remotely (similar to SSL/TLS). Thus data exchange (e.g. PIN, signed data) and the integrity of the device commands are secured.

Transport PIN

A freely selectable transport PIN allows you to secure the device while being transported to users. The transport PIN helps the user to verify that the Nitrokey HSM has not been manipulated in transit. The user must change the transport PIN to a PIN of his own choosing before using the device for the first time.

PIN Management

Nitrokey HSM provides an initialization code (SO-PIN) for device initialization security and a user PIN for secure access. The maximum number of PIN input attempts can be configured to prevent brute force attacks.

Strong Authentication

You can use a PIN or a key to authenticate. For the latter, during the initial setup of a Nitrokey HSM, register another Nitrokey HSM key. A challenge-response procedure is used when authenticating using the Nitrokey HSM.

Supported Systems and Interfaces

- X.509, S/MIME
- PKCS#11 (Public Key Cryptography Standards)
- Cryptographic Service Provider (CSP) minidriver for Windows
- C application programming interface (API)
- Java Cryptography Extension (JCE) provider
- OpenSC and Open Smart Card Development Platform (OpenSCDP)
- CA administration software: XCA, EJBCA
- GnuPG - S/MIME version
- Windows, macOS, Linux, BSD

Technical Details

- Cryptographic algorithms: RSA, ECC, AES-CBC
- Key lengths: RSA 1024-4096 bit, ECC 192-521 bit, AES 128-256 bit
- Padding/Variants: RSAES-OAEP, RSAES-PKCS1-v1_5, RSASSA-PSS, RSASSA-PKCS1-v1_5, ECDH, ECDH with HMAC KDF, ECDSA
- Elliptic curves: SECG / NIST P-192, P-256, P-384, P-521 (secp192r1/prime192v1, secp256r1/prime256v1, secp384r1/prime384v1, secp521r1/prime521v1); Bitcoin Koblitz curve: secp192k1, secp256k1, secp384k1, secp521k1; RFC 5639: brainpoolP192r1, brainpoolP224r1,brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1
- Hash algorithms: SHA-1, SHA-256, SHA-384, SHA-512, internal and external hashing supported
- Storage capacity: 76 KB EEPROM total, max. 35 x ECC-521 keys, max. 55 x ECC/AES-256 keys, max. 27 x RSA-4096 keys, max. 55 x RSA-2048 keys, max. 65536 data objects
- Performance (without 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
- Performance key generation: RSA-2048: 20 sec, RSA-4096: 120 sec, ECC-256: 6 sec, ECC-512: 8 sec
- Card Verifiable Certificates (CVC) according to BSI TR-03110 (extended access control)
- Random number generator (RNG): class DRG.3 according to AIS-20
- Encrypted backups: AES-256
- Secure messaging channel: AES-128, 3DES-112
- Life expectancy (MTBF, MTTF): > 500.000 PIN entries
- Durability USB connector (EIA-364-09): > 1,500 mate and unmate cycles
- Storage time: > 25 years
- Activity indicator: monochrome LED
- Hardware interface: USB 1.1, type A
- Maximum supply current: 50 mA
- Maximum power consumption: 250 mW
- Operating temperature: -20 °C to +70 °C
- Size: 48 x 19 x 7 mm
- Weight: 6 g
- Compliance: FCC, CE, RoHS, WEEE, OSHwA

NITROKEY IS BETTER

High Security

Your cryptographic keys will be stored securely during their entire life cycle on one or more Nitrokey HSM. From key generation, to encrypted export and import, through to use: Nitrokey HSM protects your keys against both internal and external threats. Brute force protection prevents against PIN guessing attacks by locking the device after 15 failed attempts. The security chip and the operating system used are certified according to Common Criteria EAL 5+.

Scalable Performance

A single Nitrokey HSM already meets performance requirements for offline and in-house CA (see „Technical Details“ section). You can further increase performance by using and scaling any number of Nitrokey HSM. Our PKCS#11 driver supports scaling while maintaining easy use of the cluster.

Security Requires Open Source

Both hardware and firmware, tools and libraries are open source and free software, enabling independent security audits. Flexibly adaptable, no vendor lock-in, no security through obscurity, no hidden security flaws and backdoors.[1]

Better Than Software

The Nitrokey hardware does not depend on an operating system and reliably protects your keys against theft, loss, user errors and malware.

Easy Integration

Nitrokey uses open interfaces and open source tools to enable easy integration into your systems. We can develop a customized solution for you on request. Easy connection via USB bypasses complicated installation.

Better Than Other Hardware

Unlike smart cards, Nitrokey requires no additional cables and adapters. A fully-fledged USB connector ensures easy and trouble-free connection to any standard computer and server.

Low Price

Nitrokey HSM offers high security, high quality and professional performance at a fraction of the price of a conventional HSM. Ideal for certificate infrastructures of any type and size.

Made in Berlin

Nitrokey is developed and produced in Berlin resp. Germany. For the sake of higher quality and security, we do not use cheap overseas manufacturing.

Sustainability

Regional production in Berlin, casings made from recycled plastic granulate, plastic-free shipping bags, green electricity, and refurbished laptops are examples we take for granted.

[1] Nitrokey HSM is based on SmartCard-HSM and therefore contains proprietary components of other vendors.

www.nitrokey.com

Version: 03/2022

Our Customers

1&1
ABB
adyen
arm
arvato BERTELSMANN Arvato Systems
BBC
Beiersdorf
BOSCH Invented for life
BROADCOM
BUND FRIENDS OF THE EARTH GERMANY
Bundesamt für Sicherheit in der Informationstechnik
Bundeskanzleramt
CATERPILLAR
CGI
cisco
DB
DFN CERT
Diebold Nixdorf
DIEHL
Dropbox
ERSTE Group Card Processor
Ford
Fraunhofer
FREEDOM OF THE PRESS FOUNDATION
GE Healthcare
Google
HBO
infineon
intel
Johnson & Johnson
kpn
LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
lyft
MAX PLANCK GESELLSCHAFT
Miele
moz://a
NOKIA
NVIDIA
OSD
PHILIPS
Red Hat
SAP
Schneider Electric
SENNHEISER
SIEMENS
Solarisbank
SONY
SUSE
SwissLife
T··Systems·
telenor
THALES
THE LINUX FOUNDATION
TU WIEN TECHNISCHE UNIVERSITÄT WIEN
UBS
Verifone
VHV VERSICHERUNGEN
VISA