Nitrokey
secure your digital life

NetHSM

The Trustworthy, Open Hardware Security Module That Just Works

- Secure store for cryptographic keys (e.g. web servers' TLS, DNSSEC, PKI, CA, blockchain)
- Open source allows to verify the absence of back doors
- Easy to use due to modern REST interface and modern software tools
- Made in Germany

EUROPÄISCHE UNION
Europäischer Fonds für Regionale Entwicklung
efre.brandenburg.de

The development of NetHSM was funded by the European Union within the scope of the program „Gründung innovativ" of the Investitionsbank of the German federal state Brandenburg.

FEATURES

Secure Storage of Cryptographic Keys

Store your cryptographic keys for web servers TLS, DNSSEC, PKI, and CA securely in the network-connected NetHSM hardware. Your private keys are kept secure inside the NetHSM, in case of server hacks and the physical compromise of your data center. NetHSM allows you to easily fulfill security compliance requirements.

High Security due to Open Source

Unlike proprietary HSM products, NetHSM is the first HSM available as open source, which enables independent security audits, easy customization and avoids vendor lock-in. Only open source allows to verify the absence of back doors.

Easy to Use

The modern REST interface and tools are easy to use, just as you would expect from current cloud software. NetHSM can be easily managed via its command-line software. Client systems can easily integrate the REST API using the SDKs available in 35 programming languages, or use the PKCS#11 driver. For a quick start you can access our NetHSM test server or run NetHSM as a container. Unlike other HSM vendors, all NetHSM tools, drivers, and documentation are publicly available without requiring an NDA.

Made in Germany

NetHSM is developed and built in Germany minimizing the risk of physical supply chain attacks. Skilled support personnel ensures fast issue solving.

High Performance, Availability and Scalability

A single NetHSM can handle thousands of key operations per second. NetHSM is stateless, so that several NetHSM devices can be clustered to enable extremely high throughput and high availability.

Dedicated Hardware and Cloud (Planned)

Apart from using NetHSM's dedicated hardware, NetHSM can also be deployed as container in the cloud (planned). Both deployments share the same features and interfaces.

Customizable

The NetHSM can easily be customized to meet your own specific requirements thanks to its open source architecture. We can develop a customized solution for you upon request.

ENQUERIES AND FEEDBACK

info@nitrokey.com

INNOVATIVE SECURITY ARCHITECTURE

Memory-Safe and Type-Safe Programming Language

NetHSM is not written in insecure programming languages such as C. Instead the main system is implemented from scratch in a memory-safe, type-safe, functional programming language (OCaml). This includes all levels - even the TCP/IP, HTTP, TLS and application stack. This approach ensures that a whole class of potential security vulnerabilities are excluded, namely buffer overflows and other memory access errors which generally cause 70% of all security vulnerabilities.

High Security due to Open Source

Unlike proprietary HSM products, NetHSM is the first HSM available as open source. This allows to verify the absence of back doors through independent security audits as well as easy customization and avoidance of vendor lock-in.

Small Size = Small Attack Vector

NetHSM doesn't contain an ordinary operating system, but is based on a so-called "unikernel" (MirageOS). Unikernels combine the operating system and application functionality into a specially tailored firmware that contains no unnecessary code. For example, NetHSM doesn't even contain a terminal shell and can't display to a screen. This way we achieve a very small overall system size (<50 MB) resulting in a minimal attack vector.

Formally Verified Microkernel

NetHSM contains a formally verified microkernel (Muen) for superior security. Its formal verification mathematically guarantees that the kernel doesn't contain any run-time errors. The microkernel architecture ensures that only the minimum set of required functions is provided without additional and potentially harmful functions.

Functional Separation

To ensure additional security the formally verified microkernel separates functional blocks from one another. This applies to platform device drivers, the network interface and the actual application logic. For example if attackers would manage to compromise the network driver, they won't be able to access the cryptographic keys. This is different to most ordinary operating systems in which device drivers run with root privileges.

Secure Against Physical Tampering

All cryptographic keys are being stored encrypted. This approach ensures that all keys remain securely encrypted even if attackers steal the entire device. It renders brute force attacks and hardware attacks with laboratory equipment ineffective.

ONLINE RESOURCES

www.nitrokey.com/nethsm

- Documentation
- Documentation of REST API
- Docker container image
- Command line tool
- PKCS#11 module
- Client libraries/SDKs for 50 programming languages
- Source code
- Security assessment report

TECHNICAL DETAILS

- **Cryptographic algorithms:** AES-128/192/256, ECC, RSA 1024-8192
- **Elliptic curves (ECC):** NIST P-224, P-256, P-384, P-521, Curve25519
- **Encryption ciphers:** AES CBC
- **Decryption ciphers:** AES CBC, RSA raw, RSA PKCS#1, RSA OAEP MD5/SHA1/SHA224/SHA256/SHA384/SHA512
- **Signature ciphers:** RSA PKCS#1, RSA PSS MD5/SHA1/SHA224/SHA256/SHA384/SHA512, EdDSA, ECDSA
- **Performance:**
  - NIST P-256: ~870 signatures/s, ~60 key generations/s
  - NIST P-384: ~300 signatures/s, ~55 key generations/s
  - NIST P-521: ~150 signatures/s, ~50 key generations/s
  - RSA-2048: ~740 signatures resp. decryptions/s, ~20 key generations/s
  - RSA-4096: ~120 signatures resp. decryptions/s, ~2 key generations/s
  - Ed25519: ~1370 signatures resp. decryptions/s
  - RNG: ~530 KByte/s

  These measurements include network packet round-trip time and were measured end-to-end with several parallel persistent connections.

- **Physical random number generator (TRNG):** PTG.3 according to AIS-20
- **Secure element:** TPM 2.0
- **CPU:** Intel Xeon E-2224G, 3.50 GHz, disabled Intel Management Engine
- **RAM:** 8 GB ECC, DDR4, 2666 MHz
- **Storage:** 240 GB, Intel SSD D3 with Enhanced Power Loss Data Protection and High Endurance Technology (HET)
- **Network:** 1 Gbps Ethernet
- **Power supply (PSU):** 400 W
- **Chassis:** 19" rack, 1 height unit (1U), 430 mm (W), 435 mm (D), 45 mm (H)
- **Weight:** 9 kg
- **Scope of delivery:** sealed NetHSM hardware, power cable
- **Packaging:** Individually sealed packaging

www.nitrokey.com/nethsm

Our Customers

Version: 11/2023