Nitrokey Start

The secure key for your digital life.

Encrypts your emails, files and server access. Protects against hackers and espionage – private and professional.

The cryptographic key is securely stored in the Nitrokey and is thereby protected against loss, theft and malware. With strong hardware encryption, made reliable thanks to open source, quality made in Germany.

Nitrokey
secure your digital life

USE CASES

For Anybody – Protection Against Mass Surveillance and Hackers

- **Encrypt Emails**
  Encrypt your emails with GnuPG, OpenPGP, S/MIME, Thunderbird or Outlook. Your private keys are securely stored in the Nitrokey and cannot be exported or stolen.

For Businesses, Chancelleries and the Self-Employed – Protect Sensitive Data

- **Protect Your Data Against Espionag**
  Encrypt field workers' entire hard drives by means of TrueCrypt/VeraCrypt or individual files by means of GnuPG. The private keys are thereby securely stored in the Nitrokey.

- **Desktop Login**
  Log in easily at your local computer desktop with the Nitrokey.

For IT Administrators and Security Experts – Protect Critical Infrastructure

- **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. This means that you can bypass the insecure and tedious process of synchronizing key files between client systems.

- **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.

NITROKEY IS BETTER

High Security

Your private keys are always stored in the PIN-protected Nitrokey and are as such protected against malware, loss and theft. Brute force protection prevents against PIN guessing attacks by locking the device after 6 failed attempts. The secure encryption methods RSA and ECC are supported.

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.

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.

Better Than Software

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

Complete USB Connector

Unlike some of its competitors, Nitrokey has a complete and standard-compliant USB connector. This ensures plugging the device in and out several thousand times without connection issues.

Made in Berlin

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

www.nitrokey.com

Our Customers

Supported Systems and Interfaces

- Mozilla Thunderbird, MS Outlook, GnuPG, SSH, TrueCrypt/VeraCrypt, OpenSC
- OpenPGP, S/MIME, X.509, PKCS#11
- Windows, macOS, Linux, BSD

Technical Details

- Cryptographic algorithms: RSA, ECC
- Key lengths: RSA 2048 bit, RSA 4096 bit (duration: ~ 8 sec), ECC 256 bit
- Elliptic curves: EdDSA, ECDSA (with NIST P256 and secp256k1), ECDH (with X25519, NIST P256 and secp256k1)
- Storage capacity: 3 keys (decryption, signing, authentication)
- True random number generator (TRNG)
- Life expectancy (MTBF, MTTF): > 100,000 PIN entries
- Storage time: > 20 years
- Activity indicator: two-colored LED
- Hardware interface: USB 1.1, type A
- Size: 48 x 19 x 7 mm
- Weight: 5 g
- Compliance: FCC, CE, RoHS, WEEE, OSHwA

Version: 11/2018