Nitrokey Storage 2

The secure key for your digital life.

Stores your data encrypted and secures access to your accounts. Protects against hackers and espionage – private and professional.

With Nitrokey Storage your data is stored securely encrypted and can be kept with you securely at all times. Hidden storage allows you to plausibly deny the existence of encrypted data. The Nitrokey Storage helps you to encrypt your emails and protect your accounts against identity theft. 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

- **Protect Online Accounts Against Identity Theft**
  Nitrokey is your key for secure login to websites (e.g. Google, Facebook). One-time passwords (OTP) and conventional static passwords are supported.

- **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.

- **Encrypt Files in the Mobile Storage Unit in Case of Loss**
  Carry important data around with you, always automatically hardware-encrypted in the Nitrokey Storage, independent of the operating system.

For IT Administrators and Security Experts – Protect Critical Infrastructure

- **Securely Administrating Servers With SSH**
  Securely store your SSH key 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.

For Computer Manufacturers – Protect BIOS Integrity

- Your users/customers verify the integrity of the computer BIOS with the help of Nitrokey and Verified Boot. The colored LED of the Nitrokey indicates, if the BIOS' integrity is intact (green) or a manipulation has been detected (red).

For Journalists – Source and Data Protection

- **Encrypt and Hide Data During Border Controls**
  Hide sensitive data on the Nitrokey Storage so that its existence cannot be proven. Hidden data is encrypted using an additional password and cannot be distinguished from empty storage space. By default no hidden volume is used. This allows you to plausibly deny the existence of encrypted data, for example during border controls.

- **Keep a Secure Operating System With you at all Times**
  Securely boot Linux directly from Nitrokey Storage. Nitrokey Storage protects the system against manipulation, such as the installation of surveillance software via „Evil Maid".

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

- **Protect Your Data Against Espionage**
  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.

- **Active Directory Integration**
  Roll out certificates to the Nitrokey via central Active Directory.

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

FEATURES

Hardware Encrypted Storage (16-64 GB)
Automatically encrypt your data with secure hardware encryption. Your files are protected against unauthorized access, whether you are at home, in the office, or traveling, and regardless of operating system or computer.

Hidden Storage for Highly Sensitive Data
Establish hidden volumes in order to plausibly deny the existence of additional encrypted data, for example during border controls. The hidden data is encrypted with a second, separate password and cannot be distinguished from empty storage space. By default no hidden volumes are used. This means, without the password, it is not possible to detect whether or not a hidden volume was created.

One-Time Passwords for Protecting Accounts Against Identity Theft
Protect your accounts against identity theft. One-time passwords (OTP) are generated in the Nitrokey and function as a secondary authentication factor (2FA) for logins (additional to your normal password). Thus, your accounts remain secure, even in the event that your passwords are stolen.

Secure Storage of Cryptographic Keys
Securely store your private keys for the encryption of emails, hard drives or individual files in the Nitrokey. They are thereby protected against loss, theft and malware, and can be kept with you at all times. Key backups protect against loss.

Secure Firmware Updates
Keep up-to-date with security and technology by firmware updates. Protect yourself against manipulated firmware by reviewing the authenticity and integrity of installed firmware yourself.

Password Manager
Securely store your passwords encrypted in the integrated password manager. This allows you to keep your passwords with you at all times and keep them protected even if the Nitrokey is lost.

Integrity Verification / Tamper Detection
Verify the integrity of the computer BIOS with the help of Verified Boot. The colored LED of the Nitrokey indicates, if the BIOS' integrity is intact (green) or a manipulation has been detected (red). Supported computers are required to have a BIOS based on Coreboot and Heads (e.g. Purism Librem, Insurgo PrivacyBeast, Nitrokey NitroPad).

Supported Systems and Interfaces

- Windows, Mozilla Thunderbird, MS Outlook, GnuPG, SSH, TrueCrypt/VeraCrypt, OpenSC
- CSP, OpenPGP, S/MIME, X.509, PKCS#11
- One-time passwords are compatible with the two-factor authentication of most websites (e.g. Google, Facebook, Dropbox).
  An overview of OTP-compatible websites can be found at www.dongleauth.com
- Windows, macOS, Linux, BSD

Technical Details

- Storage capacity: 16-64GB depending on the model
- Storage encryption: AES-256, CBC mode
- Secure key storage: 3 key slots, RSA 2048-4096 bit, ECC 256-512 bit. Storage capacity: 51 KB EPROM total
- Elliptic curves: NIST P-256, P-384, P-521 (secp256r1/prime256v1, secp384r1/prime384v1, secp521r1/prime521v1), brainpoolP256r1, brainpoolP384r1, brainpoolP512r1
- External hash algorithms: SHA-256, SHA-384, SHA-512
- One-time passwords: 3 x HOTP (RFC 4226), 15 x TOTP (RFC 6238), 1 x HOTP validation
- Password manager: 16 entries
- True random number generator (TRNG): 40 kbit/s
- Tamper-resistant smart card, OpenPGP Card 3.3
- Life expectancy (MTBF, MTTF): > 100,000 PIN entries
- Durability USB connector (EIA-364-09): > 1,500 mate and unmate cycles
- Storage time: > 20 years
- Activity indicator: two-colored LED
- Hardware interface: USB 2.0, type A
- Maximum supply current: 170 mA
- Maximum power consumption: 850 mW
- Size: 69 x 20 x 8 mm
- Weight: 11 g
- Compliance: FCC, CE, RoHS, WEEE, OSHwA

NITROKEY IS BETTER

High Security

Your private data and keys are always stored in the tamper-resistant and 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. RSA keys of up to 4096 bit and AES with 256 bit are supported. Nitrokey Storage has already been reviewed by an independent auditing company and found to be secure (audit reports are publicly available).

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.

No Backdoors

Installed firmware of Nitrokey Storage can be exported and verified, preventing attackers from inserting backdoors into products, for example during shipping. Nitrokey is open source and free of backdoors. All private keys are generated only by you and we have no access to your private information in the Nitrokey Storage.

Plausible Deniability

Nitrokey Storage is the only hardware solution worldwide with hidden encrypted storage. This allows you to plausibly deny the existence of encrypted data, for example during border controls.

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. Anti-twist protection reduces support costs.

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.

www.nitrokey.com

Our Customers

Version: 11/2023