Nitrokey Pro 2

The secure key for your digital life.

Encrypts your communication and secures access to your accounts. Protects against hackers and espionage – private and professional.

Nitrokey Pro helps you to encrypt your emails and files, to secure server access via SSH, and to 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.

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.

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

One-Time Passwords for Protecting Accounts Against Identity Theft

Protect your accounts against identity theft. One-time passwords are generated in the Nitrokey and function as a secondary authentication factor 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.

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.

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.info
- Windows, macOS, Linux, BSD

Technical Details

- Secure key storage: 3 x RSA 2048-4096 bit or 3 x ECC 256-521 bit, 1 x AES-128 or AES-256
- Elliptic curves: NIST P-256, P-384, P-521 (secp256r1/prime256v1, secp384r1/prime384v1, secp521r1/prime521v1), brainpoolP256r1, brainpoolP384r1, brainpoolP512r1
- 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
- Life expectancy (MTBF, MTTF): > 100,000 PIN entries
- Storage time: > 20 years
- Activity indicator: two-colored LED
- Hardware interface: USB 2.0, type A
- Size: 48 x 19 x 7 mm
- Weight: 6 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.

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

Version: 11/2018

Our Customers