Nitrokey 3

The Secure Key to Your Digital Life.
Private and Professional.

Passwordless login and two-factor authentication protect your accounts against phishing and password theft. Secure data and communication encryption. Trustworthy thanks to open source and quality made in Germany.

Nitrokey
secure your digital life

SECURE LOGIN

Two-Factor Authentication (2FA) *Becomes the Norm*

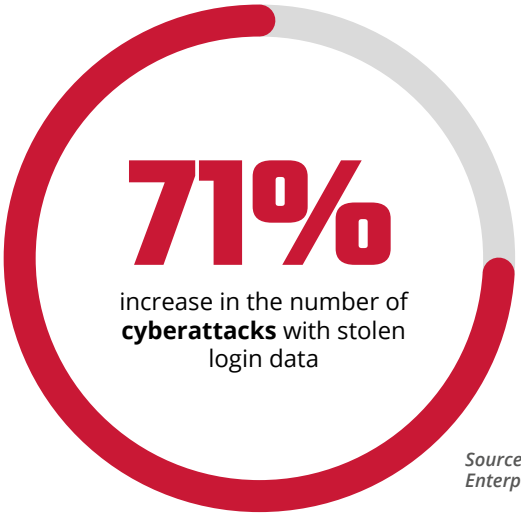
Most major websites and around half of all companies use two-factor authentication. But beware: Numerous publicly known cases prove that even SMS can be easily broken as two-factor authentication.
Thanks to strong cryptography, Nitrokey 3 supports secure two-factor authentication. This means that your accounts remain protected even if your password has been stolen.

Passwordless Login With Passkeys *Convinces*

With the Nitrokey 3, you can avoid cumbersome and insecure passwords. No more password policies, password slips of paper and forgotten passwords. From now on, you can log in easily and securely using your Nitrokey 3.
Passwordless login is two-factor authentication with device PIN. Optionally, there is no need to enter a user name. In this case, the user identifies themselves using a key on the Nitrokey 3.

Phishing Protection *is Included*

When logging in, Nitrokey 3 checks the domain and thus reliably protects you against phishing attacks.



Source: IBM Report: Identity Comes Under Attack, Straining Enterprises' Recovery Time from Breaches, 2024

15 Billion Stolen Accounts

Passwords and phishing are the most common gateways

Stolen accounts can have disastrous consequences for the people and companies affected. Weak or stolen passwords and phishing are the most common gateways for successful hacker attacks. Around 15 billion stolen accounts are currently known. You can check whether you have already been affected yourself here: https://haveibeenpwned.com https://sec.hpi.uni-potsdam.de/ilc/search

ADVANTAGES

High Acceptance Thanks to *Easy Usage*

Using the Nitrokey 3 is very simple: you configure your Nitrokey 3 once with your accounts. From then on, you confirm your login by simply pressing a button on the Nitrokey (optional: PIN entry). No additional client software or driver installation required.

Good Compatibility Due to *Future-Proof Standard*

Today, all web browsers, most popular websites and numerous on-premise web services support the required standard FIDO2 resp. Web Authentication (WebAuthn).

Nitrokey is Better

Complete USB Connector

Unlike some competitors, Nitrokey has a complete and standard-compliant USB connector. This ensures thousands of plugging cycles without connection problems. Anti-twist protection reduces support costs.

Security Requires Open Source

Both hardware and firmware are open source and enable independent security checks. Flexibly customizable, no manufacturer lock-in, no false security through obfuscation, no hidden security gaps and backdoors.

Made in Berlin

Nitrokey is developed and produced in Berlin and Germany. We avoid cheap production abroad in favor of higher quality and security.

Hardware Security

Nitrokey 3 stores your cryptographic keys in hardware so that they remain secure even if the device is lost. This makes Nitrokey 3 significantly more secure than SMS and app-based authentication methods.

Investment Security

We are continuously developing the Nitrokey 3 firmware. You receive updates and potential security corrections via software updates without having to replace the device.

Simple Integration

Nitrokey uses open interfaces and open source tools to enable easy integration into your systems. On request, we can develop a customized solution for you.

Sustainability

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

www.nitrokey.com

USE CASES

For Private and Corporate Use - Protection Against Mass Surveillance and Hackers

- **Passkeys for Passwordless Login**
  Forget your password for logging in to websites and use the Nitrokey for passwordless login instead.

- **Protect Online Accounts With Two-Factor Authentication (2FA)**
  Nitrokey is your key to secure login to websites. Using FIDO2 and one-time passwords (OTP), your accounts remain secure even if your password is stolen.

- **Phishing Protection**
  When using WebAuthn or FIDO, the respective domain is automatically checked and users are effectively protected against phishing attacks.

- **Mobile Use With Smartphones**
  You can also access your accounts securely on smartphones using passkeys and NFC.

- **Encrypting Data and E-mails**
  Encrypt your e-mails with GnuPG, OpenPGP, S/MIME, Thunderbird or Outlook. Encrypt entire hard disks with VeraCrypt, LUKS or individual files with GnuPG. Your private keys are securely stored in Nitrokey and cannot be exported/stolen.

For Companies - Protection Against Hackers and Industrial Espionage

- **Passwordless Logon to Computers**
  In future, employees will log on to their computers without passwords but with their Nitrokey.

- **Passwordless Login to Your Own Enterprise Systems**
  Replace your password policy, unauthorized password slips and time-consuming password resets with passwordless login using the Nitrokey. Security and acceptance through simplicity. We will be happy to consult you on the integration.

For IT Administrators and Security Experts - Protecting Critical Infrastructure

- **Secure Server Administration With SSH**
  Always have your SSH key securely with you in the Nitrokey. Your key is PIN-protected and cannot be exported/stolen from the Nitrokey. This eliminates the insecure and inconvenient synchronization of key files on client systems.

- **Protect Internet of Things (IoT) and Your Own Products**
  Protect your own hardware products by integrating the Nitrokey. Ideal for remote maintenance and ensuring product authenticity.

- **Securely Store Cryptographic Keys**
  Store cryptographic keys and certificates securely in the Nitrokey and prevent them from being stolen.

- **Protect BIOS Integrity of Computers**
  The Nitrokey and Measured Boot are used to verify the integrity of computer BIOS/firmware and thus protect against Evil Maid attacks. The colored LED of the Nitrokey indicates whether the BIOS is integer (green) or a tampering has been detected (red). Compatible e.g. with NitroPads and NitroPC.

FEATURES

Passkeys/WebAuthn/FIDO2 for Passwordless Login

Passkeys set new standards in terms of ease of use and thus achieve a high level of acceptance. Passkeys reliably protect your accounts against password theft and phishing.

One-time Passwords Protect Accounts Against Identity Theft

Protect your accounts against identity theft. One-time passwords are generated in the Nitrokey and serve as a second authentication factor for logins (in addition to your normal password). This ensures that your accounts remain secure even if your password is stolen.

Password Manager

Save your passwords securely encrypted in the integrated password manager. This way, you always have your passwords with you and they remain protected even if you lose your Nitrokey.

Secure Storage of Cryptographic Keys

Securely store your private keys for encrypting e-mails, hard disks or individual files in the Nitrokey. This protects them against loss, theft and computer viruses and ensures they are always with you.

Integrity Check/Tamper Detection

Verify the integrity of the computer BIOS using Measured Boot. The colored LED of the Nitrokey indicates whether the BIOS is integer (green) or a tampering has been detected (red). Supported computers require a BIOS based on Heads, such as NitroPad, NitroPC.

MODERN SECURITY TECHNOLOGY

- The entire firmware is developed in the memory-safe programming language Rust. This avoids potentially security-critical memory errors.
- Only integer, signed firmware updates can be installed.
- Nitrokey is open source, so that the secure implementation can be reviewed by anyone.
- A secure element (SE05x) is used as cryptographic storage, a kind of smart card. This has been certified up to operating system level in accordance with Common Criteria EAL 6+ and therefore meets high security requirements. Due to its power requirements, the secure element can only be used via USB but not via NFC.

TECHNICAL DETAILS

- Authentication standards: WebAuthentication (WebAuthn), CTAP2/FIDO2, CTAP1/FIDO U2F 1.2, HOTP RFC 4226, TOTP RFC 6238, HOTP verification
- Two-factor authentication using server-side credentials for an unlimited number of accounts (FIDO U2F, FIDO2)
- Smart card standards: PKCS#11 (OpenSC), Windows MiniDriver, OpenPGP Card (GnuPG), S/MIME, X.509, NIST PIV
- Secure key storage: RSA 2048-4096, NIST P-256, P-384, P-521 (secp256r1/prime256v1, secp384r1/prime384v1, secp521r1/prime521v1), Ed25519/Curve25519, Koblitz (secp256k1), brainpoolP256r1, brainpoolP384r1, brainpoolP512r1
- Performance

	Signature [ms]	Decryption [ms]
P-256	391	534
P-384	426	582
P-521	481	578
Curve25519	622	518
RSA-2048	238	240
RSA-3072	331	327
RSA-4096	465	456

- External hash algorithms: SHA-256, SHA-384, SHA-512
- Certification of the tamper-proof secure element according to CC EAL6+
- Physical random number generator (TRNG)
- With touch button
- Activity indicator: four-color LED
- Operating temperature: min. -40 °C to +80 °C
- Maximum current consumption: 30 mA
- Maximum power consumption: 150 mW
- Conformity: FCC, CE, RoHS, WEEE, OSHwA
- Supported operating systems: Windows, macOS, Linux, BSD, Android, iOS

	 **Nitrokey 3A NFC**	 **Nitrokey 3C NFC**	 **Nitrokey 3A Mini**
Passkeys	~ 30	~ 30	~ 100
Passwords	100	100	100
Plug	USB-A	USB-C	USB-A
NFC (ISO/IEC 14443)	✓	✓	
Size	48 x 19 x 7 mm	40 x 19 x 7 mm	17 x 14 x 6 mm
Weight	6 g	4 g	3 g
Lifetime (MTBF, MTTF)	> 15 years	> 15 years	> 10 years
PIN entries	> 100.000	> 100.000	> 20.000
Plugging and unplugging cycles USB plug (EIA-364-09)	> 1.500	> 10.000	> 1.500

Our Customers

Version: 04/2025