Nitrokey FIDO U2F

The secure key for your digital life.

Protects your accounts against espionage and identity theft by hackers – private and professional. With strong hardware encryption, made reliable thanks to open source, quality made in Germany.

Nitrokey
secure your digital life

HOW IT WORKS

Passwords are not Secure

Our digital identity is more important today than ever before. Correct representation on social media and in public is essential for both individuals and businesses. Moreover we can hardly forego important online services such as banking and finances. Stolen accounts can have disastrous consequences for the people affected. At the same time, successful attacks on online services and accounts are repeatedly being made public. One database currently lists over 4.7 billion stolen accounts[1]. Perpetrators also use captured usernames and passwords in order to log in with those credentials to other online services, which is why most big online services now support two-factor authentication.

Security via Two-Factor Authentication (2FA)

Nitrokey FIDO U2F is your key to secure logins to websites (e.g. Google, Facebook) and to your own systems (e.g. Nextcloud, enterprise systems). For this purpose you configure your Nitrokey FIDO U2F once with your accounts, and from that point on confirm your login by simply pushing a button on the Nitrokey. Your protected accounts remain secure even if attackers have stolen your password.

FIDO Universal 2nd Factor (U2F)

FIDO U2F impresses with its ease-of-use, versatility and high-level security. Apart from a supported web browser, no additional software or driver installation is required. Configuration and use is very easy with just the push of a button. You can use a single Nitrokey FIDO U2F to protect any number of accounts of different kinds (e.g. websites, in-house proprietary systems). Thanks to strong cryptography, FIDO U2F is significantly more secure than SMS- and app-based authentication methods.

[1]You can check if you are affected too:
https://sec.hpi.uni-potsdam.de/ilc/search
https://haveibeenpwned.com

NITROKEY IS BETTER

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.

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.

Hardware Security

Nitrokey FIDO U2F stores your cryptographic key in a cryptoprocessor so that it remains secure even if the device is stolen, and in the event of attacks using laboratory devices. Nitrokey FIDO U2F is therefore more secure than SMS- and app-based authentication methods.

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

ABB · Adobe · BBC · BOSCH Invented for life · cisco · DFN-CERT · DIEBOLD NIXDORF · DIEHL · Dropbox · GE Healthcare · Google · KUEHNE+NAGEL · moz://a · NVIDIA · OSD · redhat · SUSE · T-Systems · THE LINDE GROUP · TU WIEN · UBER · UBS · VISA

Supported Systems

- Web browser: Mozilla Firefox, Google Chrome, Safari, Chromium, Opera
- Websites: e.g. Google, Facebook, Dropbox, GitHub. Overview on www.dongleauth.info
- Windows, macOS, Linux, BSD

Technical Details

- Authentication standard: FIDO Universal 2nd Factor (U2F) 1.2
- Can be used with an unlimited number of accounts
- With touch button
- Life expectancy (MTBF, MTTF): > 20 years
- Activity indicator: monochrome 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