



Nitrokey FIDO2

Passwortloses Login und Zwei-Faktor-Authentisierung schützen Ihre Accounts privat und beruflich.

Hohe Akzeptanz und Verbreitung durch kinderleichte Bedienung und populären Standard (WebAuthentication).

Vertrauenswürdig dank Open Source Hardware made in Germany.



10 Milliarden gestohlene Accounts

Passwörter und Phishing sind häufigste Einfallstore

Gestohlene Accounts können für die betroffenen Menschen und Firmen desaströse Folgen haben. Schwache oder gestohlene Passwörter sowie Phishing sind die häufigsten Einfallstore für erfolgreiche Hacker-Angriffe. Derzeit sind ca. 10 Milliarden gestohlene Accounts bekannt. Ob Sie selber bereits betroffen sind, können Sie hier überprüfen: <https://haveibeenpwned.com>
<https://sec.hpi.uni-potsdam.de/ilc/search>

SICHERHEITSFUNKTIONEN



Zwei-Faktor-Authentisierung (2FA) *wird Normalität*

Die meisten großen Webseiten und rund die Hälfte aller Firmen verwenden Zwei-Faktor-Authentifizierung. Doch Vorsicht: Zahlreiche öffentlich bekannte Fälle belegen, dass selbst SMS als Zwei-Faktor-Authentisierung leicht zu knacken ist.

Dank starker Kryptografie unterstützt Nitrokey FIDO2 eine sichere Zwei-Faktor-Authentisierung. Somit bleiben Ihre Accounts selbst dann geschützt, wenn Ihr Passwort gestohlen wurde.



Passwortloses Login *überzeugt*

Mit dem Nitrokey FIDO2 können Sie auf umständliche und unsichere Passwörter verzichten. Keine Passwort-Policies, Passwort-Zettel und vergessene Passwörter mehr. Von nun an melden Sie sich kinderleicht und sicher mittels Ihres Nitrokey FIDO2 an Windows 10 Pro, an Microsoft Office 365 und an eigenen Enterprise-Diensten an.

Bei passwortlosem Login handelt es sich um Zwei-Faktor-Authentisierung mit Geräte-PIN. Optional, sofern von der Webseite unterstützt, kann auf die Eingabe eines Benutzernamens verzichtet werden. Hierbei identifiziert sich der Benutzer anhand eines Schlüssels auf dem Nitrokey FIDO2.



Phishing-Schutz *ist inklusive*

Beim Login überprüft Nitrokey FIDO2 die Domain und schützt Sie somit zuverlässig gegen Phishing Angriffe.



VORTEILE

+ Hohe Akzeptanz durch kinderleichte Bedienung

Die Nutzung des Nitrokey FIDO2 ist denkbar einfach: Sie konfigurieren Ihren Nitrokey FIDO2 einmalig mit Ihren Accounts. Von nun an bestätigen Sie Ihr Login durch einen simplen Knopfdruck auf den Nitrokey (optional: PIN-Eingabe). Neben einem gängigen Webbrowser ist keine zusätzliche Client-Software oder Treiberinstallation nötig.

+ Gute Kompatibilität durch zukunfts-sicheren Standard

Alle gängigen Webbrowser unterstützen bereits den erforderlichen Standard FIDO2 bzw. Web-Authentication (WebAuthn). Zunehmend wird WebAuthn von Webseiten (z. B. Google, Facebook), von On-Premise-Webdiensten (z. B. Nextcloud) und auch von Windows 10 Pro (mit Azure Active Directory) zur Desktop-Anmeldung unterstützt.

+ Vertrauen durch Open Source Hardware Made in Germany

Nitrokey FIDO2 ist zwecks Transparenz als Open Source Hardware veröffentlicht und wird vollständig in Deutschland produziert.



ANWENDUNGSFÄLLE

FÜR PRIVAT – *Schutz gegen Hacker*

- **Online-Accounts mittels Zwei-Faktor-Authentisierung schützen**

Nitrokey ist Ihr Schlüssel zum sicheren Login an Webseiten (z. B. Google, Facebook; Übersicht auf www.dongleauth.com). Sie können einen einzigen Nitrokey FIDO2 zur Absicherung beliebig vieler Accounts verwenden.

- **Passwortlose Anmeldung**

Vergessen Sie Ihr Passwort zur Anmeldung an Microsoft-Diensten (z. B. Microsoft Office 365) und verwenden Sie stattdessen den Nitrokey FIDO2 zum passwortlosen Login.

FÜR FIRMEN – *Schutz gegen Hacker und Industriespionage*

- **Online-Accounts mittels Zwei-Faktor-Authentisierung schützen**

Nitrokey ist Ihr Schlüssel zum sicheren Login an Webseiten (z. B. Google, Facebook; Übersicht auf www.dongleauth.com). Sie können einen einzigen Nitrokey FIDO2 zur Absicherung beliebig vieler Accounts verwenden.

- **Passwortlose Anmeldung an eigenen Enterprise-Systemen**

Ersetzen Sie Ihre Passwort-Policy, unerlaubte Passwort-Zettel und aufwendiges Passwort-Reset durch passwortloses Login mit dem Nitrokey FIDO2. Sicherheit und Akzeptanz durch Einfachheit. Wir beraten Sie gerne bei der Integration.

- **Passwortlose Anmeldung**

Vergessen Sie Ihr Passwort zur Anmeldung an Microsoft-Diensten (z. B. Microsoft Office 365) und verwenden Sie stattdessen den Nitrokey FIDO2 zum passwortlosen Login.

- **Passwortlose Anmeldung an lokalen Windows 10 Computern**

Mitarbeiter melden sich zukünftig an ihre, mittels Azure Active Directory verwalteten, Windows 10 Pro Computer ohne Passwörter an. Dazu ist lediglich ein Nitrokey FIDO2 nötig.



Unterstützte Systeme

- Webbrowser: Mozilla Firefox, Google Chrome, Safari, Microsoft Edge, Chromium, Opera
- Webseiten: z. B. Google, Facebook, Dropbox, GitHub. Übersicht auf www.dongleauth.com
- Windows, macOS, Linux, BSD



Technische Details

- Authentifizierungsstandards: WebAuthentication (WebAuthn), CTAP2/FIDO2, CTAP1/FIDO U2F 1.2
- Zwei-Faktor-Authentisierung und passwortlose Anmeldung für unbegrenzte Anzahl von Accounts (FIDO U2F, FIDO2)
- Anmeldung ohne Benutzernamen für 50 Accounts (FIDO2)
- Signierte Firmware-Aktualisierungen
- Mit Touchbutton
- Aktivitätsanzeige: dreifarbige LED
- Lebensdauer (MTBF, MTTF): > 20 Jahre
- Lebensdauer USB-Stecker (EIA-364-09): > 1.500 Steck- und Absteckzyklen
- Hardware-Schnittstelle: USB 1.1, Typ A
- Maximale Stromaufnahme: 10 mA
- Maximale Leistungsaufnahme: 500 mW
- Größe: 48 x 19 x 7 mm
- Gewicht: 5 g
- Konformität: FCC, CE, RoHS, WEEE, OSHwA



NITROKEY IST BESSER



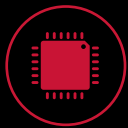
Sicherheit erfordert Open Source

Sowohl Hardware als auch Firmware sind Open Source und ermöglichen unabhängige Sicherheitsüberprüfungen. Flexibel anpassbar, keine Herstellerabhängigkeit, keine Schein-Sicherheit durch Verschleierung, keine versteckten Sicherheitslücken und Hintertüren.



Vollständiger USB-Stecker

Anders als manche Mitbewerber verfügt Nitrokey über einen vollständigen und standardkonformen USB-Stecker. Dadurch sind tausende von Steckvorgängen ohne Verbindungsprobleme sichergestellt. Verdreh-sicherheit reduziert Supportaufwände.



Hardware-Sicherheit

Nitrokey FIDO2 speichert Ihren kryptografischen Schlüssel in Hardware, so dass dieser auch bei Verlust des Geräts sicher bleibt. Dadurch ist Nitrokey FIDO2 deutlich sicherer als SMS- und App-basierte Authentifizierungsverfahren.



Made in Berlin

Nitrokey wird in Berlin bzw. Deutschland entwickelt und produziert. Zugunsten höherer Qualität und Sicherheit verzichten wir auf eine billige Herstellung im Ausland.



Einfache Integration

Nitrokey verwendet offene Schnittstellen und Open Source Tools, um die einfache Integration in Ihre Systeme zu ermöglichen. Auf Wunsch entwickeln wir eine angepasste Lösung für Sie.



Nachhaltigkeit

Regionale Produktion in Berlin, Gehäuse aus recyceltem Plastikgranulat, plastikfreie Versandtaschen, Ökostrom und generalüberholte Laptops sind für uns selbstverständliche Beispiele.

www.nitrokey.com

Unsere Kunden

