Nitrokey 3

Der sichere Schlüssel zu Ihrem digitalen Leben. *Privat und beruflich.*

Passwortloses Login und Zwei-Faktor-Authentisierung schützen Ihre Accounts gegen Phishing und Passwort-Diebstahl. Sichere Daten- und Kommunikations-Verschlüsselung. Vertrauenswürdig dank Open Source und Qualität made in Germany.

Nitrokey
secure your digital life

SICHERES LOGIN

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

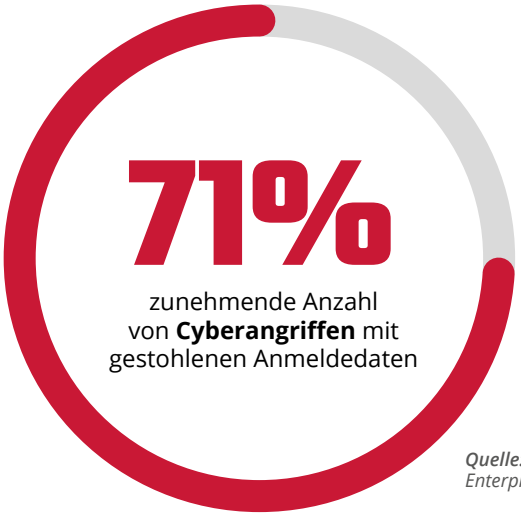
Die meisten großen Webseiten und rund die Hälfte aller Firmen verwenden Zwei-Faktor-Authentifizierung. Doch Vorsicht: Zahlreiche öffentlich bekannte Fälle belegen, dass selbst SMS als Zwei-Faktor-Authentisierung leicht zu knacken ist.
Dank starker Kryptografie unterstützt Nitrokey 3 eine sichere Zwei-Faktor-Authentisierung. Somit bleiben Ihre Accounts selbst dann geschützt, wenn Ihr Passwort gestohlen wurde.

Passwortloses Login mit Passkeys *überzeugt*

Mit dem Nitrokey 3 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 3 an.
Bei passwortlosem Login handelt es sich um Zwei-Faktor-Authentisierung mit Geräte-PIN. Optional kann auf die Eingabe eines Benutzernamens verzichtet werden. Hierbei identifiziert sich der Benutzer anhand eines Schlüssels auf dem Nitrokey 3.

Phishing-Schutz *ist inklusive*

Beim Login überprüft Nitrokey 3 die Domain und schützt Sie somit zuverlässig gegen Phishing Angriffe.



15 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. 15 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

VORTEILE

Hohe Akzeptanz durch *kinderleichte Bedienung*

Die Nutzung des Nitrokey 3 ist denkbar einfach: Sie konfigurieren Ihren Nitrokey 3 einmalig mit Ihren Accounts. Von nun an bestätigen Sie Ihr Login durch einen simplen Knopfdruck auf den Nitrokey (optional: PIN-Eingabe). Keine zusätzliche Client-Software oder Treiberinstallation erforderlich.

Gute Kompatibilität durch *zukunftssicheren Standard*

Heutzutage unterstützen alle Webbrowser, die meisten populären Webseiten und zahlreiche On-Premise-Webdienste den erforderlichen Standard FIDO2 bzw. Web-Authentication (WebAuthn).

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

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.

Hardware-Sicherheit

Nitrokey 3 speichert Ihre kryptografischen Schlüssel in Hardware, so dass dieser auch bei Verlust des Geräts sicher bleibt. Dadurch ist Nitrokey 3 deutlich sicherer als SMS- und App-basierte Authentifizierungsverfahren.

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.

www.nitrokey.com

Vollständiger USB-Stecker

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

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.

Investitionssicherheit

Wir entwickeln die Nitrokey 3 Firmware kontinuierlich weiter. Sie erhalten Aktualisierungen und potentielle Sicherheitskorrekturen per Software-Update, ohne dass ein Geräteaustausch nötig ist.

Nachhaltigkeit

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

ANWENDUNGSFÄLLE

Für privat und Unternehmen – Schutz gegen Massenüberwachung und Hacker

- **Passkeys zur passwortlosen Anmeldung**
  Vergessen Sie Ihr Passwort zur Anmeldung an Webseiten und verwenden Sie stattdessen den Nitrokey zum passwortlosen Login.

- **Online-Accounts mittels Zwei-Faktor-Authentisierung (2FA) schützen**
  Nitrokey ist Ihr Schlüssel zum sicheren Login an Webseiten. Mittels FIDO2 und Einmalpasswörtern (OTP) bleiben Ihre Accounts auch dann sicher, falls Ihr Passwort gestohlen wird.

- **Phishing-Schutz**
  Bei der Verwendung von WebAuthn bzw. FIDO wird die jeweilige Domain automatisch überprüft und die Benutzer effektiv gegen Phishing-Angriffe geschützt.

- **Mobile Nutzung mit Smartphones**
  Mittels Passkeys und NFC können Sie auch an Smartphones sicher auf Ihre Accounts zugreifen.

- **Daten und E-Mails verschlüsseln**
  Verschlüsseln Sie Ihre E-Mails mit GnuPG, OpenPGP, S/MIME, Thunderbird oder Outlook. Verschlüsseln Sie gesamte Festplatten mittels VeraCrypt, LUKS oder einzelne Dateien mittels GnuPG. Ihre privaten Schlüssel werden sicher im Nitrokey gespeichert und können nicht exportiert/gestohlen werden.

Für Firmen – Schutz gegen Hacker und Industriespionage

- **Passwortlose Anmeldung an Computern**
  Mitarbeiter melden sich zukünftig an ihren Computern ohne Passwörter sondern mit ihrem Nitrokey an.

- **Passwortlose Anmeldung an eigenen Enterprise-Systemen**
  Ersetzen Sie Ihre Passwort-Policy, unerlaubte Passwort-Zettel und aufwendiges Passwort-Reset durch passwortloses Login mit dem Nitrokey. Sicherheit und Akzeptanz durch Einfachheit. Wir beraten Sie gerne bei der Integration.

Für IT-Administratoren und Sicherheitsexperten – kritische Infrastruktur schützen

- **Server sicher mit SSH administrieren**
  Haben Sie Ihren SSH-Schlüssel immer sicher im Nitrokey dabei. Ihr Schlüssel ist PIN-geschützt und kann nicht aus dem Nitrokey exportiert/gestohlen werden. Somit entfällt das unsichere und lästige Synchronisieren von Schlüsseldateien auf Clientsystemen.

- **Internet of Things (IoT) und eigene Produkte schützen**
  Schützen Sie Ihre eigenen Hardware-Produkte durch Integration des Nitrokeys. Ideal zur Fernwartung und zur Gewährleistung der Produktechtheit.

- **Kryptographische Schlüssel sicher speichern**
  Speichern Sie kryptographische Schlüssel und Zertifikate sicher im Nitrokey und verhindern so deren Diebstahl.

- **BIOS-Integrität von Computern schützen**
  Mittels des Nitrokey und Measured Boot wird die Integrität von Computer-BIOS/Firmware überprüft und somit gegen Evil Maid Angriffe geschützt. Die farbige LED des Nitrokey signalisiert, ob das BIOS integer ist (grün) oder eine Manipulation erkannt wurde (rot). Kompatibel z.B. mit NitroPads und NitroPC.

FUNKTIONEN

Passkeys/WebAuthn/FIDO2 zum passwortlosem Login

Bei der einfachen Benutzbarkeit setzen Passkeys neue Maßstäbe und erzielen somit hohe Akzeptanz. Passkeys schützen Ihre Accounts zuverlässig gegen Passwortdiebstahl und gegen Phishing.

Einmalpasswörter schützen Accounts gegen Identitätsdiebstahl

Schützen Sie Ihre Accounts gegen Identitätsdiebstahl. Einmalpasswörter werden im Nitrokey generiert und dienen als zweiter Authentifizierungsfaktor für Logins (zusätzlich zu Ihrem normalen Passwort). Somit bleiben Ihre Accounts auch bei gestohlenem Passwort sicher.

Passwortmanager

Speichern Sie Ihre Passwörter sicher verschlüsselt im integrierten Passwortspeicher. So haben Sie Ihre Passwörter immer dabei und sie bleiben auch bei Verlust des Nitrokeys geschützt.

Sichere Speicherung kryptografischer Schlüssel

Speichern Sie Ihre privaten Schlüssel für die Verschlüsselung von E-Mails, Festplatten oder einzelnen Dateien sicher im Nitrokey. So sind diese gegen Verlust, Diebstahl und Computerviren geschützt und immer dabei.

Integritätsüberprüfung/Manipulationserkennung

Überprüfen Sie die Integrität vom Computer-BIOS mittels Measured Boot. Die farbige LED des Nitrokey signalisiert, ob das BIOS integer ist (grün) oder eine Manipulation erkannt wurde (rot). Unterstützte Computer erfordern ein BIOS auf Basis von Heads, wie z.B. das NitroPad, NitroPC.

MODERNE SICHERHEITSTECHNOLOGIE

- Die gesamte Firmware ist in der speichersicheren Programmiersprache **Rust** entwickelt. Dadurch werden potentiell sicherheitskritische Speicherfehler vermieden.
- Nur integre, signierte Firmware-Aktualisierungen können installiert werden.
- Nitrokey ist **open source**, so dass die sichere Implementierung von jedem begutachtet werden kann.
- Als kryptographischer Speicher wird ein **Sicherheitselement** (Secure Element SE05x) verwendet, quasi eine Chipkarte. Dieses wurde bis zur Betriebssystem-Ebene nach **Common Criteria EAL 6+** zertifiziert und entspricht somit hohen Sicherheitsanforderungen. Aufgrund des Strombedarfs kann das sichere Element nur per USB aber nicht per NFC verwendet werden.

TECHNISCHE DETAILS

- Authentifizierungsstandards: WebAuthentication (WebAuthn), CTAP2/FIDO2, CTAP1/FIDO U2F 1.2, HOTP RFC 4226, TOTP RFC 6238, HOTP-Prüfung
- Zwei-Faktor-Authentisierung mittels Server-Side Credentials für unbegrenzte Anzahl von Accounts (FIDO U2F, FIDO2)
- Chipkartenstandards: PKCS#11 (OpenSC), Windows MiniDriver, OpenPGP Card (GnuPG), S/MIME, X.509, NIST PIV
- Sicherer Schlüsselspeicher: RSA 2048-4096, NIST P-256, P-384, P-521 (secp256r1/prime256v1, secp384r1/prime384v1, secp521r1/prime521v1), Ed25519/Curve25519, Koblitz (secp256k1), brainpoolP256r1, brainpoolP384r1, brainpoolP512r1
- Geschwindigkeit

	Signatur [ms]	Entschlüsselung [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

- Externe Hash-Algorithmen: SHA-256, SHA-384, SHA-512
- Zertifizierung des manipulationsgeschützten Sicherheitselement nach CC EAL6+
- Physikalischer Zufallszahlengenerator (TRNG)
- Mit Touchbutton
- Aktivitätsanzeige: vierfarbige LED
- Betriebstemperatur: min. -40 °C bis +80 °C
- Maximale Stromaufnahme: 30 mA
- Maximale Leistungsaufnahme: 150 mW
- Konformität: FCC, CE, RoHS, WEEE, OSHwA
- unterstützte Betriebssysteme: Windows, macOS, Linux, BSD, Android, iOS

	 **Nitrokey 3A NFC**	 **Nitrokey 3C NFC**	 **Nitrokey 3A Mini**
Passkeys	~ 30	~ 30	~ 100
Passwörter	100	100	100
Stecker	USB-A	USB-C	USB-A
NFC (ISO/IEC 14443)	✓	✓	
Größe	48 x 19 x 7 mm	40 x 19 x 7 mm	17 x 14 x 6 mm
Gewicht	6 g	4 g	3 g
Lebensdauer (MTBF, MTTF)	> 15 Jahre	> 15 Jahre	> 10 Jahre
PIN-Eingaben	> 100.000	> 100.000	> 20.000
Steck- und Absteckzyklen USB-Stecker (EIA-364-09)	> 1.500	> 10.000	> 1.500

Unsere Kunden

Stand: 04/2025