Nitrokey Storage 2

Der sichere Schlüssel zu Ihrem digitalen Leben.

Speichert Ihre Daten verschlüsselt und sichert Zugriffe auf Ihre Accounts. Schützt gegen Hacker und Spionage – privat und beruflich.

Mit dem Nitrokey Storage sind Ihre Daten sicher verschlüsselt gespeichert und auch mobil immer sicher dabei. Mit einem versteckten Speicher können Sie die Existenz verschlüsselter Daten glaubhaft abstreiten. Der Nitrokey Storage hilft Ihnen, Ihre E-Mails zu verschlüsseln und Ihre Accounts gegen Identitätsdiebstahl abzusichern. Mit starker Hardware-Verschlüsselung, vertrauenswürdig dank Open Source, Qualität made in Germany.

Nitrokey
secure your digital life

ANWENDUNGSFÄLLE

Für jeden – Schutz gegen Massenüberwachung und Hacker

- **Online-Accounts gegen Identitätsdiebstahl schützen**
  Nitrokey ist Ihr Schlüssel zum sicheren Login an Webseiten (z. B. Google, Facebook). Es werden Einmalpasswörter (OTP) und gewöhnliche statische Passwörter unterstützt.

- **E-Mails verschlüsseln**
  Verschlüsseln Sie Ihre E-Mails mit GnuPG, OpenPGP, S/MIME, Thunderbird oder Outlook. Ihre privaten Schlüssel werden sicher im Nitrokey gespeichert und können nicht exportiert/gestohlen werden.

- **Dateien im mobilen Speicher für Verlustfall verschlüsseln**
  Tragen Sie wichtige Daten mit sich herum – immer automatisch hardwareverschlüsselt im Nitrokey Storage und unabhängig vom Betriebssystem.

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.

Für Computer-Hersteller - BIOS-Integrität schützen

- Ihre Benutzer/Kunden überprüfen mittels des Nitrokey und Verified Boot die Integrität des Computer-BIOS. Die farbliche LED des Nitrokey signalisiert, ob das BIOS integer ist (grün) oder eine Manipulation erkannt wurde (rot).

Für Journalisten – Quellen- und Datenschutz

- **Daten bei Grenzkontrollen verschlüsseln und verstecken**
  Verstecken Sie sensible Dateien auf dem Nitrokey Storage, so dass deren Existenz nicht nachgewiesen werden kann. Versteckte Daten sind mit einem zusätzlichen Passwort verschlüsselt und vom leeren Speicherbereich nicht zu unterscheiden. Standardmäßig wird kein verstecktes Volumen verwendet. Dies ermöglicht Ihnen, glaubhaft die Existenz von verschlüsselten Daten abzustreiten, z. B. bei Grenzkontrollen.

- **Ein sicheres Betriebssystem immer dabei**
  Starten Sie ein sicheres Linux direkt vom Nitrokey Storage. Der Nitrokey Storage schützt das System vor Manipulationen (z. B. Einbau von Überwachungssoftware durch „Evil Maid“).

Für Unternehmen, Kanzleien und Selbstständige – sensible Daten schützen

- **Datenschutz gegen Spionage**
  Verschlüsseln Sie gesamte Festplatten von Außendienstmitarbeitern mittels TrueCrypt/VeraCrypt oder einzelne Dateien mittels GnuPG. Dabei werden die privaten Schlüssel sicher im Nitrokey gespeichert.

- **Active Directory Integration**
  Rollen Sie Zertifikate auf den Nitrokey mittels zentralem Active Directory aus.

- **Desktop-Login**
  Melden Sie sich an Ihrem lokalen Computer-Desktop unkompliziert mit dem Nitrokey an.

FUNKTIONEN

Hardwareverschlüsselter Speicher (16-64 GB)
Verschlüsseln Sie Ihre Daten automatisch mit sicherer Hardware-Verschlüsselung. Somit sind Ihre Dateien zuhause, im Büro und auf Reisen gegen unbefugten Zugriff geschützt, unabhängig vom Betriebssystem oder Computer.

Versteckter Speicher für besonders sensible Daten
Richten Sie versteckte Volumen ein, um z. B. bei Grenzkontrollen glaubhaft die Existenz zusätzlicher verschlüsselter Daten abstreiten zu können. Die versteckten Daten sind mit einem weiteren Passwort verschlüsselt und vom leeren Speicherbereich nicht zu unterscheiden. Standardmäßig wird kein verstecktes Volumen verwendet. Somit kann ohne das Passwort nicht erkannt werden, ob ein verstecktes Volumen eingerichtet wurde oder nicht.

Einmalpasswörter zum Schutz von Accounts gegen Identitätsdiebstahl
Schützen Sie Ihre Accounts gegen Identitätsdiebstahl. Einmalpasswörter (OTP) werden im Nitrokey generiert und dienen als zweiter Authentifizierungsfaktor (2FA) für Logins (zusätzlich zu Ihrem normalen Passwort). Somit bleiben Ihre Accounts auch bei gestohlenem Passwort sicher.

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. Schlüsselbackups schützen gegen Verlust.

Sichere Firmware-Updates
Bleiben Sie mit Firmware-Updates auf dem neuesten Stand von Sicherheit und Technik. Schützen Sie sich gegen manipulierte Firmware, indem Sie die Authentizität und Integrität der installierten Firmware selbst überprüfen.

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

Integritätsüberprüfung/Manipulationserkennung
Überprüfen Sie die Integrität vom Computer-BIOS mittels Verified Boot. Die farbliche LED des Nitrokey signalisiert, ob das BIOS integer ist (grün) oder eine Manipulation erkannt wurde (rot). Unterstützte Computer erfordern ein BIOS auf Basis von Coreboot und Heads (z.B. Purism Librem, Insurgo PrivacyBeast, Nitrokey NitroPad).

Unterstützte Systeme und Schnittstellen

- Windows, Mozilla Thunderbird, MS Outlook, GnuPG, SSH, TrueCrypt/VeraCrypt, OpenSC
- CSP, OpenPGP, S/MIME, X.509, PKCS#11
- Einmalpasswörter sind kompatibel zur Zwei-Faktor-Authentifizierung der meisten Webseiten (z. B. Google, Facebook, Dropbox). Übersicht OTP-kompatibler Webseiten auf www.dongleauth.com
- Windows, macOS, Linux, BSD

Technische Details

- Speicherplatz: je nach Modell 16-64 GB
- Speicherverschlüsselung: AES-256, CBC-Modus
- Sicherer Schlüsselspeicher: 3 Schlüssel, RSA 2048-4096 Bit, ECC 256-512 Bit. Speicherkapazität: 51 KB EEPROM insgesamt
- Elliptische Kurven: NIST P-256, P-384, P-521 (secp256r1/prime256v1, secp384r1/prime384v1, secp521r1/prime521v1), brainpoolP256r1, brainpoolP384r1, brainpoolP512r1
- Externe Hash-Algorithmen: SHA-256, SHA-384, SHA-512
- Einmalpasswörter: 3 x HOTP (RFC 4226), 15 x TOTP (RFC 6238), 1 x HOTP-Prüfung
- Passwortmanager: 16 Einträge
- Physikalischer Zufallszahlengenerator (TRNG): 40 kbit/s
- Manipulationsgeschützte Chipkarte, OpenPGP Card 3.3
- Lebensdauer (MTBF, MTTF): > 100.000 PIN-Eingaben
- Lebensdauer USB-Stecker (EIA-364-09): > 1.500 Steck- und Absteckzyklen
- Speicherdauer: > 20 Jahre
- Aktivitätsanzeige: zweifarbige LED
- Hardware-Schnittstelle: USB 2.0, Typ A
- Maximale Stromaufnahme: 170 mA
- Maximale Leistungsaufnahme: 850 mW
- Größe: 69 x 20 x 8 mm
- Gewicht: 11 g
- Konformität: FCC, CE, RoHS, WEEE, OSHwA

NITROKEY IST BESSER

Hohe Sicherheit

Ihre privaten Daten und Schlüssel werden immer im manipulationssicheren und PIN-geschützten Nitrokey gespeichert und somit gegen Computerviren, Verlust und Diebstahl geschützt. Schutz gegen Brute-Force-Angriffe verhindert das Erraten der PIN, indem das Gerät nach 6 Fehlversuchen gesperrt wird. RSA-Schlüssel bis zu 4096 Bit und AES mit 256 Bit werden unterstützt. Nitrokey Storage wurde bereits durch ein unabhängiges Audit-Unternehmen geprüft und für sicher befunden (Prüfungsberichte öffentlich einsehbar).

Sicherheit erfordert Open Source

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

Keine Hintertüren

Die Firmware des Nitrokey Storage kann exportiert und überprüft werden. Dies vereitelt das Einschleusen von Hintertüren (Backdoors), z. B. während des Versands. Nitrokey Storage ist Open Source und enthält keine Hintertüren. Alle privaten Schlüssel werden von Ihnen generiert, so dass wir keinen Zugriff auf Ihre privaten Daten im Nitrokey Storage haben.

Glaubhafte Abstreitbarkeit

Nitrokey Storage ist die einzige Hardware-Lösung weltweit mit verschlüsseltem und verstecktem Speicher. Dies ermöglicht Ihnen, glaubhaft die Existenz von verschlüsselten Daten abzustreiten, z. B. bei Grenzkontrollen.

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.

Besser als Software

Die Nitrokey-Hardware ist betriebssystemunabhängig und schützt Ihre Daten und Schlüssel zuverlässig gegen Diebstahl, Verlust, Benutzerfehler und Computerviren.

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.

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

Stand: 09/2024