Datenblatt

Nitrokey Pro 2

Numero Ordine:	NK-PRO
Hersteller:	Nitrokey
Herkunftsland:	Deutschland
Zolltarifnummer:	84718000
Gewicht:	0.009 kg

Der sichere Schlüssel zu Ihrem digitalen Leben.
Verschlüsselt Ihre Kommunikation und sichert Zugriffe auf Ihre Accounts. Schützt gegen Hacker und Spionage – privat und beruflich. Der Nitrokey Pro hilft Ihnen, Ihre E-Mails, Festplatten und Dateien zu verschlüsseln, Server-Zugriffe per SSH zu sichern und Ihre Accounts gegen Identitätsdiebstahl abzusichern. Mit starker Hardware-Verschlüsselung, vertrauenswürdig dank Open Source, Qualität made in Germany.

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.

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.

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.

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).

Funktionen

- **Einmalpasswörter zum Schutz von 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.
- **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.
- **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 vwww.dongleauth.info
- Windows, macOS, Linux, BSD

Technische Details

- Sicherer Schlüsselspeicher: 3 x RSA 2048-4096 Bit oder 3 x ECC 256-521 Bit, 1 x AES-128 oder AES-256
- 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
- Speicherdauer: > 20 Jahre
- Aktivitätsanzeige: zweifarbige LED
- Hardware-Schnittstelle: USB 1.1, Typ A
- Maximale Stromaufnahme: 50 mA
- Maximale Leistungsaufnahme: 250 mW
- Größe: 48 x 19 x 7 mm
- Gewicht: 6 g

Weitere Bilder:

Datenblatt