Datenblatt

Nitrokey 3A Mini

Artikel-Nr.:	NK-3AMINI
Hersteller:	Nitrokey
Herkunftsland:	Deutschland
Zolltarifnummer:	84718000
Gewicht:	0.009 kg

Der neue Nitrokey 3 ist der beste Nitrokey den wir je entwickelt haben. Er bietet erstmals USB-A Mini. Der Nitrokey 3 vereint die Funktionen vorheriger Nitrokey Modelle: FIDO2, Einmalpasswörter, OpenPGP Chipkarte, Curve25519, Passwort-Manager, Common Criteria EAL 6+ zertifiziertes Secure Element, Firmware-Updates. Damit werden Ihre Accounts zuverlässig gegen Phishing und Passwort-Diebstahl geschützt und Ihre Kommunikation und Daten verschlüsselt. Mit starker Hardware-Verschlüsselung, vertrauenswürdig dank Open Source, Qualität made in Germany.

WICHTIGER HINWEIS !!!
Das ausgelieferte Gerät unterstützt FIDO2 und FIDO U2F und beinhaltet bereits die Hardware (inkl. Secure Element) für alle aufgeführten Funktionen. Weitere Funktionen wie Einmalpasswörter, Passwortmanager und OpenPGP Chipkarte werden nicht zum Auslieferungszeitpunkt implementiert sein, sondern später per Firmware-Updates bereitgestellt.

Anwendungsfälle
Für privat und Unternehmen - Schutz gegen Massenüberwachung und Hacker

- **Passwortlose Anmeldung**
  Vergessen Sie Ihr Passwort zur Anmeldung an Microsoft-Diensten (z. B. Office 365) und Nextcloud 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 (z. B. Google, Facebook; Übersicht auf www.dongleauth.com. Mittels FIDO2, FIDO U2F, oder Einmalpasswörtern (OTP) bleiben Ihre Accounts auch dann sicher, falls Ihr Passwort gestohlen werden sollte.
- **Phishing-Schutz**
  Bei der Verwendung von FIDO wird die jeweilige Domain automatisch überprüft und die Benutzer effektiv gegen Phishing-Angriffe geschützt.
- **Daten und E-Mails verschlüsseln**
  Verschlüsseln Sie Ihre E-Mails mit GnuPG, OpenPGP, S/MIME, Thunderbird oder Outlook. Verschlüsseln Sie gesamte Festplatten mittels TrueCrypt/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 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 3 nötig.
- **Passwortlose Anmeldung an eigenen Enterprise-Systemen**
  Ersetzen Sie Ihre Passwort-Policy, unerlaubte Passwort-Zettel und aufwendiges Passwort-Reset durch passwortloses Login mit dem Nitrokey 3. 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 des Computer-BIOS/Firmware überprüft und somit gegen Evil Maid Angriffe geschützt. Die farbliche LED des Nitrokey signalisiert, ob das BIOS integer ist (grün) oder eine Manipulation erkannt wurde (rot). Kompatibel z.B. mit NitroPads.

Funktionen

- **FIDO U2F, FIDO2 zum passwortlosem Login**
  Bei der einfachen Benutzbarkeit setzt FIDO neue Maßstäbe und erzielt somit hohe Akzeptanz. FIDO schützt Ihre Accounts zuverlässig gegen Passwortdiebstahl und gegen Phishing.
- **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 wie z.B. das NitroPad.

Sicherheitstechnologie
Der Nitrokey 3 basiert auf einer neuartigen Sicherheitsarchitektur:

- Die gesamte Firmware ist in der speichersicheren Programmiersprache Rust entwickelt. Dadurch werden potentiell sicherheitskritische Speicherfehler vermieden.
- Die Firmware basiert auf dem in Rust entwickelten Framework Trussed, welches für sicherheitskritische Embedded-Systeme ausgelegt ist und in Zusammenarbeit mit unserem Partner Solokey entwickelt wird. Trussed realisiert u.a. kryptographische Operationen. Natürlich ist der Code als Open Source veröffentlicht.
- Die Hardware basiert auf dem Mikroprozessor LPC55S6x oder nRF52, welcher über zahlreiche Sicherheitsfunktionen verfügt, wie z.B. Secure Boot, ARM TrustZone, Physical Unclonable Functions (PUF).
- Zusätzlich wird für den kryptographischen Speicher ein Secure Element (SE050), quasi eine Chipkarte, verwendet. Dieses wurde bis zur Betriebssystem-Ebene nach Common Criteria EAL 6+ sicherheitszertifiziert und entspricht somit auch hohen Sicherheitsanforderungen.

- Wie bei allen Entwicklungen von Nitrokey, ist auch der Nitrokey 3 open source, so dass die sichere Implementierung von jedem begutachtet werden kann.

Unterstützte Systeme und Schnittstellen

- Betriebssysteme: Windows, macOS, Linux, BSD
- Schnittstellen: Microsoft CSP, OpenPGP, S/MIME, X.509, PKCS#11, OpenSC, FIDO2, FIDO U2F
- Übersicht einiger Webseiten mit Zweifaktorauthentisierung auf www.dongleauth.com

Technische Details

- Authentifizierungsstandards: WebAuthentication (WebAuthn), CTAP2/FIDO2, CTAP1/FIDO U2F 1.2, HMAC-Based One-Time Password (RFC 4226), Time-Based One-Time Password (RFC 6238)
- Zwei-Faktor-Authentisierung und passwortlose Anmeldung für unbegrenzte Anzahl von Accounts (FIDO U2F, FIDO2)
- Signierte Firmware-Aktualisierungen
- Mit Touchbutton
- Zertifzierung des manipulationsgeschützten Sicherheitselement nach CC EAL6+
- Sicherer Schlüsselspeicher: RSA 2048-4096 Bit oder ECC 256-521 Bit, AES-128 oder AES-256
- Elliptische Kurven: NIST P-256, P-384, P-521 (secp256r1/prime256v1, secp384r1/prime384v1, secp521r1/prime521v1), Ed25519/Curve25519, Koblitz (192-256 Bit), brainpoolP256r1, brainpoolP384r1, brainpoolP512r1
- Externe Hash-Algorithmen: SHA-256, SHA-384, SHA-512
- Einmalpasswörter: HOTP (RFC 4226), TOTP (RFC 6238), HOTP-Prüfung
- Physikalischer Zufallszahlengenerator (TRNG)
- Aktivitätsanzeige: vierfarbige LED
- Hardware-Schnittstellen: USB 1.1, Typ A

Weitere Bilder: