Nitrokey Start

Der sichere Schlüssel zu Ihrem digitalen Leben.

Verschlüsselt Ihre E-Mails, Dateien und Server/SSH-Zugriffe. Schützt gegen Hacker und Spionage – privat und beruflich.

Dabei wird der kryptografische Schlüssel sicher im Nitrokey gespeichert und ist gegen Verlust, Diebstahl und Computerviren geschützt. 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

- **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 Unternehmen, Kanzleien und Selbstständige – sensible Daten schützen

- **Datenschutz gegen Spionage**
  Verschlüsseln Sie einzelne Dateien von Außendienstmitarbeitern mittels GnuPG. Dabei werden die privaten Schlüssel sicher im Nitrokey gespeichert.

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

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.

NITROKEY IST BESSER

Hohe Sicherheit

Ihre privaten Schlüssel werden immer im 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. Die sicheren Verschlüsselungsverfahren RSA und ECC werden unterstützt.

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.

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 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

1&1, ABB, ABN·AMRO, adyen, amazon, AON, arm, arvato BERTELSMANN, BANG & OLUFSEN, BBC, Beiersdorf, BOSCH Invented for life, BROADCOM, BUND, Bundesamt für Sicherheit in der Informationstechnik, Bundeskanzleramt, CANONICAL, CATERPILLAR, CGI, CISCO, Danfoss, DB, dm TECH, dpd, DFN-CERT, Diebold Nixdorf, DIEHL, Dropbox, EnBW, ERICSSON, ERSTE Group Card Processor, Ford, Fraunhofer, FREEDOM OF THE PRESS FOUNDATION, FUJIFILM, GE Healthcare, gematik, Google, GROUPON, HBO, here, Infineon, ingenico, intel, Johnson&Johnson, KPMG, kpn, LMU, logitech, lyft, MAX PLANCK GESELLSCHAFT, Miele, mozilla, NOKIA, NRK, NVIDIA, OSD, PHILIPS, PHOENIX CONTACT, python SOFTWARE FOUNDATION, SAP, Red Hat, Revolut, ROBERT KOCH INSTITUT, ROHDE&SCHWARZ, Schneider Electric, secunet, SENNHEISER, shopify, SIEMENS, Solarisbank, SONY, SUSE, SwissLife, T, TCS TATA CONSULTANCY SERVICES, telenor, THALES, TOMTOM, T-Systems, THE LINUX FOUNDATION, TU WIEN TECHNISCHE UNIVERSITÄT WIEN, UBS, Vaillant, verifone, VHV VERSICHERUNGEN, VISA, ZEISS

Unterstützte Systeme und Schnittstellen

- Mozilla Thunderbird, MS Outlook, GnuPG, SSH, TrueCrypt/VeraCrypt, OpenSC
- OpenPGP, S/MIME, X.509, PKCS#11
- Windows, macOS, Linux, BSD

Technische Details

- Kryptografiealgorithmen: RSA, ECC
- Schlüssellängen: RSA 2048 Bit, RSA 4096 Bit (Dauer: ca. 8 Sekunden), ECC 256 Bit
- Elliptische Kurven: EdDSA, ECDSA (mit NIST P256 und secp256k1), ECDH (mit X25519, NIST P256 und secp256k1)
- Externe Hash-Algorithmen: MD5, RIPEMD-160, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- Speicherkapazität: 3 Schlüssel (Entschlüsselung, Signatur, Authentifizierung)
- Konform zur OpenPGP Card 2 mit ECC-Unterstützung
- Physikalischer Zufallszahlengenerator (TRNG)
- Lebensdauer (MTBF, MTTF): > 100.000 PIN-Eingaben
- Lebensdauer USB-Stecker (EIA-364-09): > 1.500 Steck- und Absteckzyklen
- Speicherdauer: > 20 Jahre
- Aktivitätsanzeige: einfarbige LED
- Hardware-Schnittstelle: USB 1.1, Typ A
- Maximale Stromaufnahme: 40 mA
- Maximale Leistungsaufnahme: 200 mW
- Betriebstemperatur: -20 °C bis +70 °C
- Größe: 48 x 19 x 7 mm
- Gewicht: 5 g
- Konformität: FCC, CE, RoHS, WEEE, OSHwA

Stand: 09/2024