# Crypto Stick

## Datensicherheit mittels Open Source USB Stick


# Einleitung

Der Crypto Stick ist ein USB Stick mit integrierter, proprietärer Chipkarte zur hochsicheren Verschlüsselung von e-Mails und Daten, zur Benutzerauthentifikation in Netzwerken und zur Zugangskontrolle. Anders als bei Softwarelösungen werden die Schlüssel immer sicher im Crypto Stick gespeichert. Es ist unmöglich diese auszulesen, so dass der Crypto Stick immun gegen Computerviren und sog. „Trojaner“ ist. Die durch den Benutzer gewählte PIN und die manipulationssichere Architektur schützen im Falle von Verlust und Diebstahl. Hardware und Software sind als Open Source verfügbar, um die Überprüfung der Sicherheit und die Integration in eigene Anwendungen zu ermöglichen.

### Anwendungsfälle:

- E-Mail-Verschlüsselung basierend auf X.509 / S/MIME und OpenPGP (z.B. Outlook, Thunderbird, Evolution).
- Verschlüsselung von Daten auf separaten Speichermedien (z.B. TrueCrypt).
- Benutzer-Authentifikation auf lokalen Computern (z.B. Windows, Linux).
- Benutzer-Authentifikation für Netzwerk-Dienste (z.B. Firefox, OpenSSL, OpenVPN, IPSec, OpenID).

### Vorteile gegenüber normalen Softwarelösungen:

- Geheime Schlüssel sind immer im Crypto Stick gespeichert. Ihr Auslesen ist unmöglich. Alle sensiblen kryptografischen Operationen werden im Crypto Stick berechnet.
- Benutzer-gewählte PIN schützt im Falle von Verlust und Diebstahl gegen Brute-Force-Angriffe.
- Immun gegen Computer-Viren, Trojaner, Phishing-Angriffe und andere schädliche Software.
- Manipulationssicheres Design verhindert hochentwickelte physische Angriffe mit Laborgeräten.
- Geheime Schlüssel werden sicher auf dem Crypto Stick erzeugt, um deren Auslesen durch Angreifer zu verhindern.

### Vorteile gegenüber proprietären Sicherheitsgeräten:

- Sichere Implementierung kann vom Benutzer und unabhängigen Dritten überprüft werden, um sicherzustellen dass keine Hintertüren und Sicherheitslücken existieren.

- Kompatibel zu einer Vielzahl von Software-Anwendungen wie zum Beispiel MS Outlook, GnuPG, Enigmail, Mozilla Thunderbird, OpenSSH.
- Aufgrund offener Schnittstellen und offener Treiber sind eigene Anwendungen leicht integrierbar.
- Fehlender Hersteller Lock-in erhöht die Sicherheit ihrer Investition.
- Es werden keine Geheimnisse beim Hersteller gespeichert, von denen die Sicherheit abhängt.
- Wachsende Akzeptanz und Nutzerbasis unterstützt die kontinuierliche Verbesserung und sorgt für eine hohe Sicherheit durch Peer-Reviews.
- Transparenter und offener Entwicklungsprozess im Rahmen eines Open-Source-Projekts.

## Weitere Vorteile:

- Kompatibel zu Windows, Linux und MacOS X.
- Zusätzliche Administrator-PIN ermöglicht hierarchisches Sicherheitsmanagement .
- Drei unabhängige RSA-Schlüssel, maximale Länge 4096 Bit.
- Das Importieren vorhandener Schlüssel und Backup von Schlüsseln ist möglich.
- Hohe Sicherheit durch integrierte Chipkarte, die auf Common Criteria 5-hoch Zertifizierung basiert.

## Viele verbreitete Sicherheits- und Verschlüsselungsgeräte wurden bisher geknackt:

- 2011 wurde RSA Inc gehackt und geheime Informationen über **RSAs securID Token** gestohlen, welches erlaubte diese Token zu knacken.[1]
- 2010 wurde bekannt, dass auf mit AES-256 verschlüsselte und **FIPS 140-2 Level 2 zertifizierte** USB Speicher der folgenden Hersteller einfach mittels Standardpasswort zugegriffen werden konnte:[2] **Kingston, SanDisk, Verbatim, MXI, PICO**
- zahlreiche weitere Produkte[3]

## In Entwicklung befindliche Features:

- verschlüsselter portabler Massenspeicher, basierend auf AES-256
- OATH zur sicheren Anmeldung (z.B. bei Google Anwendungen)

## Wir unterstützen Sie bei der Integration in Ihre Anwendungen und Produkte.

1 http://www.wired.com/threatlevel/2011/03/rsa-hacked/
2 http://www.zdnet.com/blog/hardware/encryption-busted-on-nist-certified-kingston-sandisk-and-verbatim-usb-flash-drives/6655
3 http://heise.de/-1641184
http://www.youtube.com/watch?v=Yc95myrnQ0E&NR=1
http://www.schneier.com/blog/archives/2010/03/crypto_implemen.html
http://h-online.com/-746225
http://heise.de/-270060
http://heise.de/-270702
http://secunia.com/advisories/12522/

# www.crypto-stick.com

---

## Über die German Privacy Foundation

Der Crypto Stick wird von dem gemeinnützigen Verein German Privacy Foundation e.V. (GPF) gefördert. Die GPF bietet kostenlose Benutzerunterstützung und stellt die kontinuierliche Entwicklung des Crypto Sticks sicher. Außerdem bietet sie Schulungen und Beratungsleistungen an.

**Kontakt:**

German Privacy Foundation, Berliner Str. 69, 13189 Berlin, Germany, www.privacyfoundation.de