



БУДЬ НА ЧЕКУ,  
В ТАКИЕ ДНИ  
ПОДСЛУШИВАЮТ СТЕНЫ.  
НЕДАЛЕКО ОТ БОЛТОВНИ  
И СПЛЕТНИ  
ДО ИЗМЕНЫ.

**НЕ БОЛТАЙ!**



Aus dem russischen übersetzt  
Von Heidi Selig, Engelsdorf



БУДЬ НА ЧЕКУ,  
В ТАКИЕ ДНИ  
ПОДСЛУШИВАЮТ СТЕНЫ.  
НЕДАЛЕКО ОТ БОЛТОВНИ  
И СПЛЕТНИ  
ДО ИЗМЕНЫ.

**НЕ БОЛТАЙ!**



Quelle:  
[https://bettercrypto.org/static/  
applied-crypto-hardening.pdf](https://bettercrypto.org/static/applied-crypto-hardening.pdf)

**Herzlich Willkommen!**

# **Smartcards**

**CRYPTO für die Hosentasche?**

# Reiner SCT



- OWOK
- One Web – One Key

Diese Vorteile bietet Ihnen die loginCard

- Sicherer Zugang zu Ihrer kostenlosen Online-Festplatte
- Komfortable Anmeldung an Ihrem Computer
- Sicherer Zugriff auf Ihre geschützten Ordner und Dokumente
- Login bei vielen Internet-Diensten via Allyve.de
- Gratis Garantieverlängerung fürs REINER SCT Kartenlesegerät
- Zukunftssicher: Weitere Anwendungen in Vorbereitung

**OWOK**  
reiner-sct.com/owok

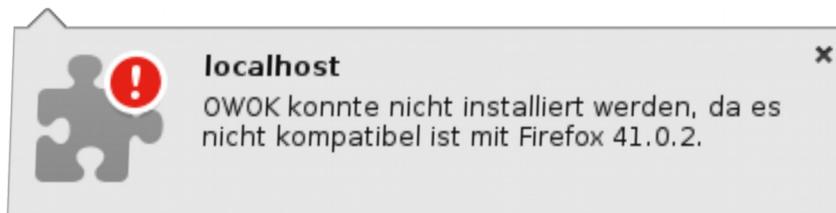
Die loginCard nutzt die OWOK-Technologie. OWOK ist Freeware & ermöglicht sicheres Kartenlogin in beliebigen Anwendungen.

The image shows a yellow and black advertisement for the loginCard. It lists several benefits and includes the OWOK logo and website information.

- SDK ist freie Software
- SDK dummerweise nicht kompatibel zu modernen PCs

# Reiner SCT - OWOK

- Reine login card
- Beigabe bei Kauf eines Kartenlesegeräts  
Ich konnte die Karte zur Garantieverlängerung des Lesers benutzen
- Voraussetzung 32bit PC + Firefox ESR17
- OWOK ist Freeware, SDK kostenlos erhältlich
- Aktuelle Version ist 1.08 vom 1.08.2011



Aktuelle Fehlermeldung

# Feitian – ein chinesischer Produzent



- RSA Keys mit 2048 Bit
- Bis zu 7 Zertifikate
- PKCS15 compliant

- PIN +
- PUK +
- SO-PIN -



# Feitian – PKI Card

**\$> pkcs15-tool -D**

Using reader with a card: Feitian SCR301 00 00

PKCS#15 Card [Reinhard Mutz]:

- Version : 0
- Serial number : 1653372118220212
- Manufacturer ID: EnterSafe
- Last update : 20150825120522Z
- Flags : EID compliant
  
- PIN [User PIN]
  - Object Flags : [0x3], private, modifiable
  - ID : 01
  - Flags : [0x32], local, initialized, needs-padding
  - Length : min\_len:4, max\_len:16, stored\_len:16
  - Pad char : 0x00
  - Reference : 1 (0x01)
  - Type : ascii-numeric
  - Path : 3f005015

- Private RSA Key [CAcert WoT User]

Object Flags : [0x3], private, modifiable

Usage : [0x12C], sign, signRecover, unwrap, derive

Access Flags : [0xD], sensitive, alwaysSensitive,  
neverExtract

- ModLength : 2048
- Key ref : 1 (0x1)
- Native : yes
- Path : 3f005015
- Auth ID : 02
- ID : 58dcc9e12b9332a0858cef7f11b992f7fd7d2551
- MD:guid : {6dd359f7-064f-f929-82ef-e94199d35c71}
- :cmap flags : 0x0
- :sign : 0
- :key-exchange: 0
  
- X.509 Certificate [CAcert WoT User]
  - Object Flags : [0x2], modifiable
  - Authority : no
  - Path : 3f0050153100
  - ID : 58dcc9e12b9332a0858cef7f11b992f7fd7d2551
  - Encoded serial : 02 02 50B1

# GnuPG Card

Version 2.0

- RSA Key Length 3072 Bit
- Verlangt die Installation der ccid udev rules.
- Begrenzter Speicherplatz



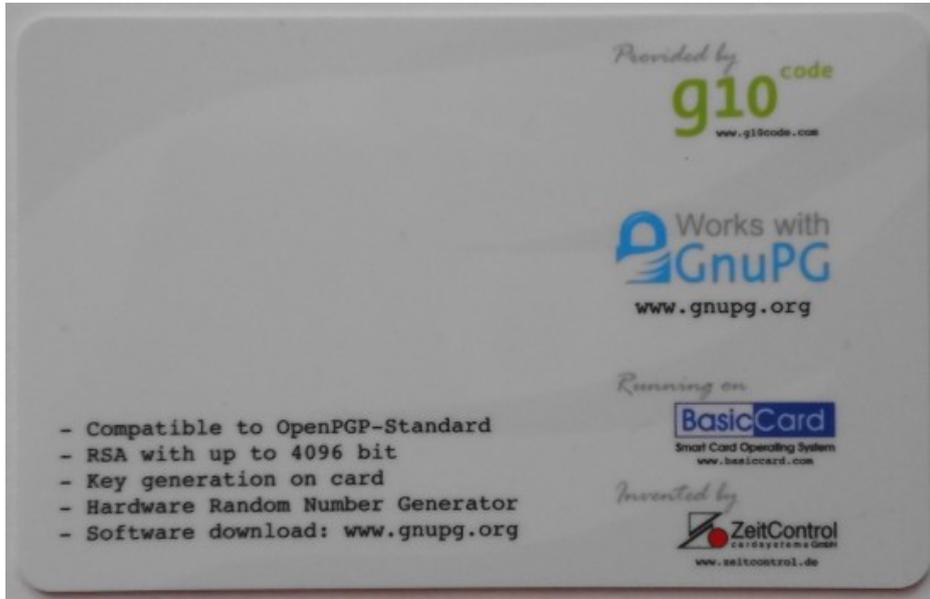
# GnuPG Card - Datenstruktur

- > **gpg2 --card-status**

- Application ID ....: D276000124010200000500001EA60000
- Version .....: 2.0
- Manufacturer .....: ZeitControl
- Serial number ....: 00001EA6
- Name of cardholder: Reinhard Mutz
- Language prefs ....: de
- Sex .....: männlich
- URL of public key : [nicht gesetzt]
- Login data .....: [nicht gesetzt]
- Signature PIN ....: zwingend
- Key attributes ...: 2048R 2048R 2048R
- Max. PIN lengths .: 32 32 32
- PIN retry counter : 3 0 3
- Signature counter : 0
- Signature key ....: [none]
- Encryption key....: [none]
- Authentication key: [none]
- General key info.: [none]
- 

- Karte erhältlich bei [kernelconcepts.de](http://kernelconcepts.de)
- Dokumentation der Karten gibt es bei <http://g10code.com/p-card.html>

# GnuPG Card



- Version 2.1
- RSA Key Length 4096 Bit
- Verbesserungen gegenüber Version 2.0
- Technische Beschreibung der Version 3.0 vorhanden – die Karte noch nicht

# Reader



- z.B. R301 von Feitian
- [http://ftsafe.com/product/Smart\\_Reader/R301C25](http://ftsafe.com/product/Smart_Reader/R301C25)
- USB 2.0 Full Speed Device
- Supports ISO-7816-1/2/3 T=0 and T=1 Protocol
- Supports ISO-7816 Class A,B and C Cards

# Feitian - Epass2003

- USB Crypto Stick



- Nur Windows

# SCM Reader



- Der kleinste Reader,
- Den ich gefunden habe
  
- Klein und handlich
- Foto von [amazon.de](https://www.amazon.de)

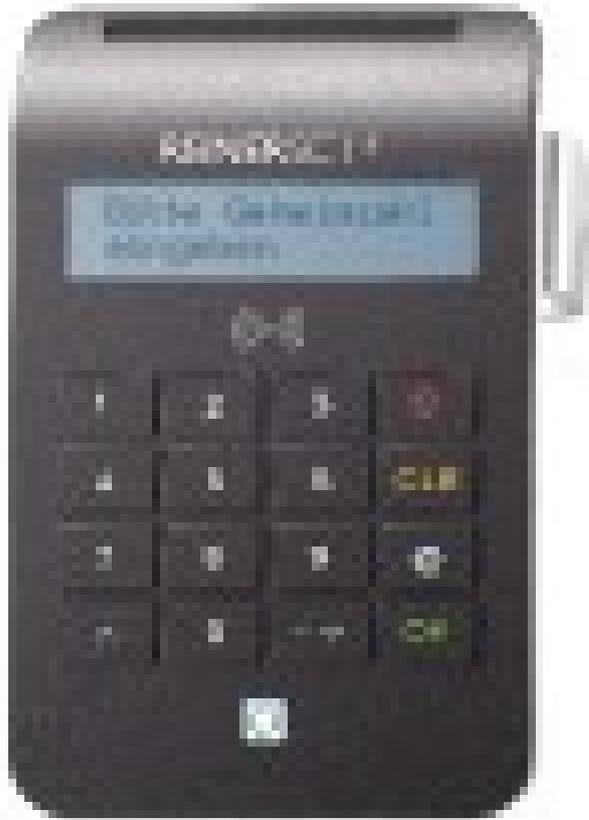
# SCM Reader

- USB 2.0

- Quelle:  
[amazon.de](https://www.amazon.de)



# Lesegeräte von Reiner SCT



- Komfortleser von Reiner SCT
- Für kontaktbehaftete und kontaktlose (NPA) Karten
- Quelle:  
[www.reiner-sct.com](http://www.reiner-sct.com)

## **Installation unter Linux, hier OpenSUSE 13.2**

Es werden die beiden Pakete OpenSC und GnuTLS benötigt. Wichtig: Das Paket OpenSC sollte  $\geq 13.0$  sein.

Aktuell sind die Versionen `opensc-0.14.0-44.2.x86_64` und `gnutls-3.2.18-8.1.x86_64`.

Reader und Smartcards funktionieren „out of the box“, sofern diese OpenSC unterstützen.

## ***Digitales Zertifikat erzeugen***

- **ein Schlüsselpaar erzeugen**
- **ein Certificate Signing Request erzeugen**
- **auf dem Testserver von CAcert einloggen**
- **den CSR hochladen**
- **das Zertifikat erzeugen und herunter laden**
- **Zertifikat und Schlüssel im Format \*.p12 abspeichern**
  
- **Das fertige Zertifikat kann jetzt in Anwendungen wie Browser, Emailclient u.a. importiert werden.**
- **Es geht allerdings auch auf eine Smartcard!**

# ein Schlüsselpaar erzeugen

Mittels openssl:

```
openssl genrsa -out client.key 4096
```

anzeigen mit certtool:

```
certtool -k < client.key
```

Mittels certtool:

```
certtool --generate-privkey --outfile key01.pem --ecc
```

anzeigen mit certtool:

```
certtool -k < client.key
```

# ein Certificate Signing Request erzeugen

## create certificate signing request

## all empty fields enter '.' a simple dot

```
openssl req -new -key client.key -out cert.csr
```

```
certtool --crq-info < cert.csr
```

# Zertifikat und Schlüssel im Format \*.p12 abspeichern

Es muss das Zertifikat zusammen mit dem Schlüsselpaar in eine Datei überführt werden. Damit diese Datei später in Emailclients verwendet werden kann, ist das Format P12 erforderlich.

Also

```
openssl pkcs12 -export -out rm-  
SERIENNUMMER.p12 -inkey client.key -in  
mycert.pem -name "rmSERIENNUMMER"
```

# Firefox - Kryptomodul

- Das vollständige Zertifikat im Format P12 kann nun auf eine Smartcard gebracht werden
- Die Smartcard mit `pkcs15-init -E` initialisieren
- Siehe Manpage von `pkcs15-init`
- Bei Firefox im Menue  
Einstellungen → Erweitert → Kryptographiemodule →  
Button „Laden“
- Name vergeben und Modul angeben
- Eintrag auswählen, dann anmelden

# Firefox - Kryptomodule

Kryptographie-Modul-Manager

Sicherheitsmodule und -einrichtu...

- ▼NSS Internal PKCS #11 Module
  - Allgemeine Krypto-Dienste
  - das Software-Sicherheitsmodul
- ▼rockey
  - Virtual hotplug slot
  - Unnamed Slot
- ▼Eingebaute Wurzelmodule
  - Builtin Object Token
- ▼testmodul
  - Virtual hotplug slot
  - Reinhard Mutz (User PIN)**

Details	Wert
Status	Nicht eingeloggt
Beschreibung	Feitian SCR301 00 00
Hersteller	OpenSC (www.opensc-proje...
HW-Version	0.0
FW-Version	0.0
Etikett	Reinhard Mutz (User PIN)
Hersteller	EnterSafe
Seriennummer	1618342118220212
HW-Version	0.0
FW-Version	0.0

Anmelden (Log In)

Abmelden (Log Out)

Passwort ändern

Laden

Entladen

FIPS aktivieren

OK

# Smartcards im Unternehmen

- No Eyesdropping
- Passwort vergessen? Fehlanzeige!
- Passwort am Telefon weitergeben? Fehlanzeige!
- Smartcards im Unternehmenseinsatz
- Mitarbeiter kennt nur die PIN
- Mit der PUK wird die Anzahl der Fehlversuche auf 0 zurückgesetzt
- Die SO-PIN (Security Officer Pin) erlaubt das Setzen eines neuen Passworts
- OpenVPN, Email sind typische Einsatzgebiete

# Smartcards zu Hause?

- Wo kann man besser den Umgang mit Krypto Hardware trainieren?
- Wo erfährt man besser die Schwachstellen der zukünftigen Entwicklungen?
- Wissen ist Macht!
- Ver- und Entschlüsselung passiert nur auf der Karte

# Danke für die Aufmerksamkeit

- Fragen? Jetzt oder auf der Mailingliste von [gaos.org](http://gaos.org)

- “Security is a process, not a product.”

Bruce Schneier