



**GERMAN
PRIVACY
FOUNDATION e.V.**

1.7.2011, Jan Suhr

Problem: Do You Trust Your Internet Cafe?



Problem: Do You Trust Your Internet Service Provider?

Intercept your e-mails,
chat, social websites

→ Encryption
e.g. GnuPG

Track your web surfing
Censor the Internet

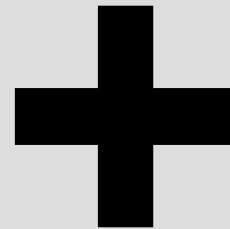
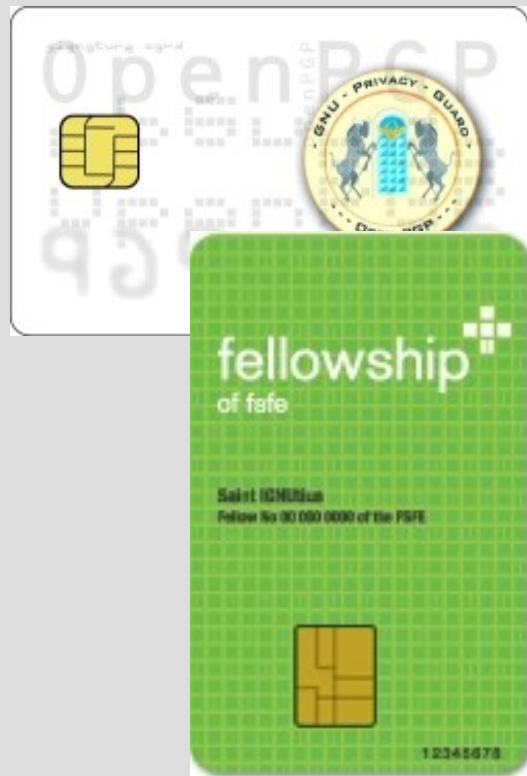
→ Tor,
Jondonym



GERMAN
PRIVACY
FOUNDATION e.V.

Solution: Security Token

OpenPGP
Card v2



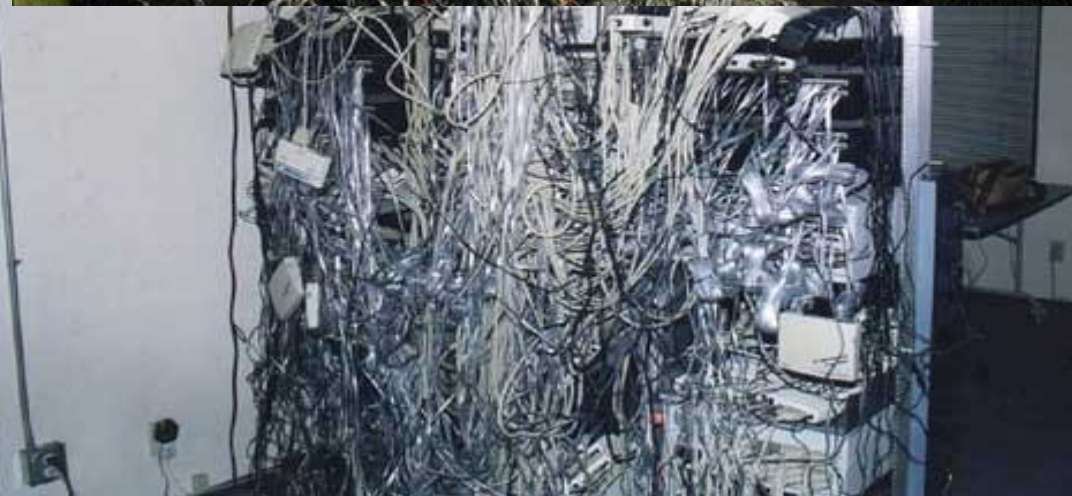
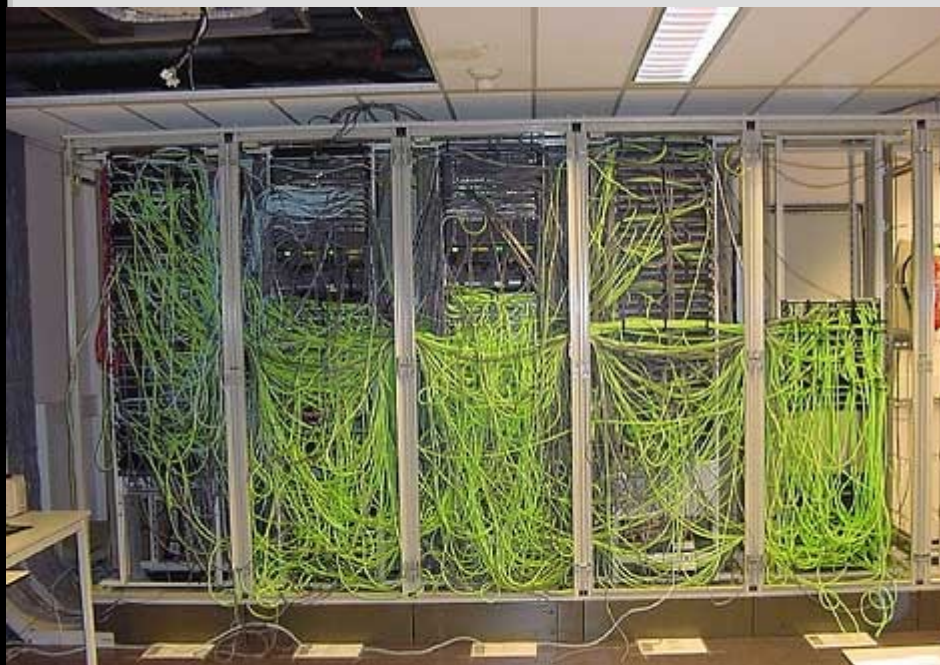
Smartcard
adapter



GERMAN
PRIVACY
FOUNDATION e.V.

A New Problem: Smartcard reader

Oh no, not another device!



GPF Crypto Stick



www.crypto-stick.com



GERMAN
PRIVACY
FOUNDATION e.V.

What is it for? To Protect!

Protects your private keys against:

- Key logger, trojan horses, computer viruses
- Thieves
- Lost
- User mistakes



GERMAN
PRIVACY
FOUNDATION e.V.

Use Cases

- E-mail encryption
- File encryption
- Authentication
- Secure connections



Features

- USB interface
- No ordinary storage!
- Secure key storage
- Encryption functionality
- PIN-protected
- Compatible to OpenPGP and X.509
- Open Source: software, hardware interface!



Features – in Detail

- Contains the OpenPGP smartcard v2
- Based on Common Criteria certification
- Key generation on stick
- 3 independent keys (for authentication, encryption, signature)
- RSA key length up to 4096 bit
- Extensible firmware



Compatible Applications

- Linux, Windows, Mac OS
- GnuPG, Thunderbird+Enigmail, Evolution, MS Outlook
- SSH, OpenVPN
- Linux authentication
- TrueCrypt, Thunderbird, Firefox, PKCS#11 compliant



GERMAN
PRIVACY
FOUNDATION e.V.

Email Encryption

The screenshot displays the Thunderbird email client interface. The top toolbar includes a 'Message' menu and a 'Nachricht verschlüsseln' (Encrypt message) button, which is currently active. The 'Add-Ins' menu is open, showing the 'OpenPGP' sub-menu. The 'OpenPGP' menu is expanded, showing options such as 'Entschlüsseln/Überprüfen', 'Automatisch entschlüsseln/überprüfen', and 'SmartCard verwalten...'. The email composition window shows the recipient as 'cryptostick@privacyfoundation.de' and the subject as 'Hallo'. The left sidebar shows the folder structure, including 'Posteingang (1)' and 'Lokale Ordner'. The bottom right corner shows the 'Konten' (Accounts) section.

Hallo - Message (HTML)

Message Insert Options Format Text Add-Ins

Nachricht verschlüsseln
/ Nachricht signieren

Menu Commands Toolbar Commands

To... cryptostick@privacyfoundation.de;
Cc...
Bcc...
Subject: Hallo

Hallo,

markuserherd@techmetrik.de - Thunderbird

Datei Bearbeiten Ansicht Navigation Nachricht OpenPGP Extras Hilfe

Abrufen Verfassen Adressbuch Entschlüsseln

Alle Ordner

- markuserherd...hmetrik.de
 - Posteingang (1)
 - Gesendet
 - Papierkorb
 - Lokale Ordner
 - Posteingang
 - Postausgang
 - Entwürfe
 - Gesendet
 - Papierkorb

Thunderbird

E-Mail

- Nachricht
- Neue Nachricht

Konten

- Konten-Einstellungen bearbeiten

OpenPGP menu items:

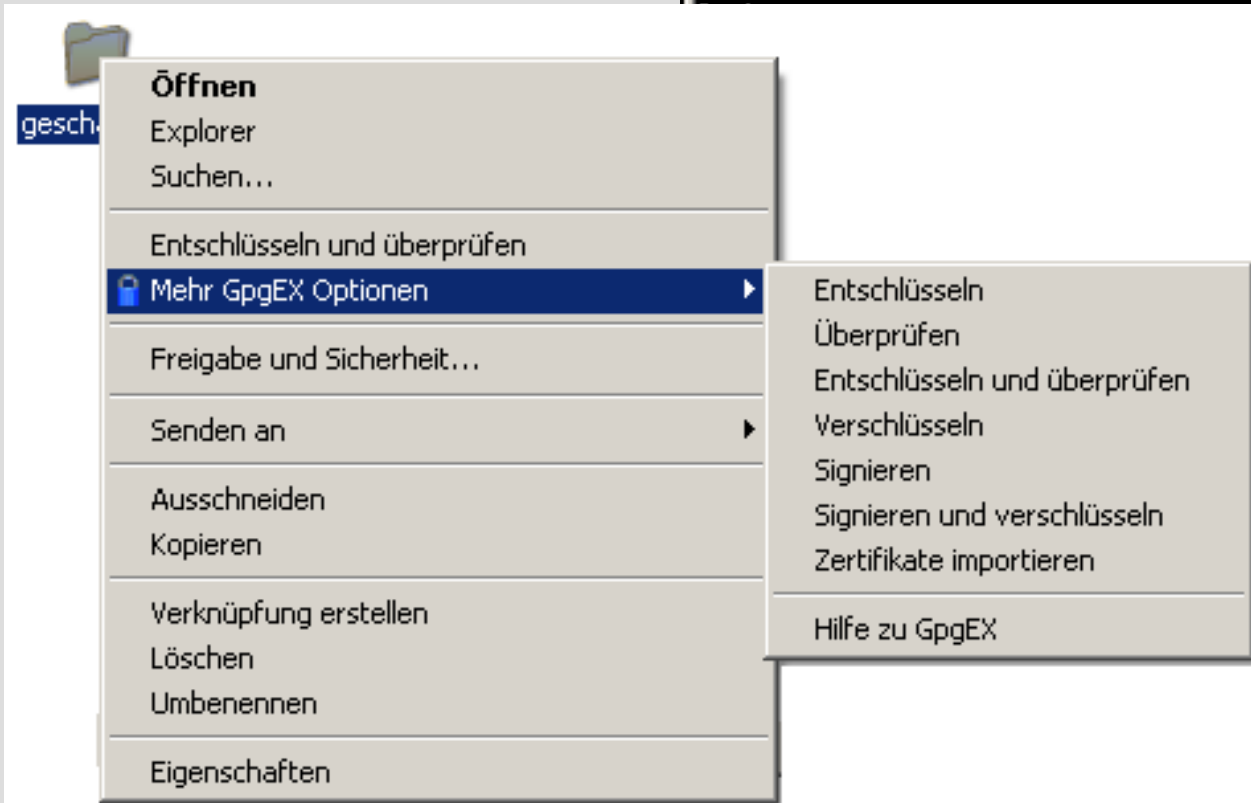
- Entschlüsseln/Überprüfen
- Entschlüsselte Nachricht speichern
- Automatisch entschlüsseln/überprüfen
- Passphrase aus Cache löschen
- Nachricht neu laden
- Schlüssel des Absenders
- Einstellungen...
- Empfängerregeln...
- Schlüssel verwalten...
- SmartCard verwalten...
- Fehlersuche
- Hilfe
- Über OpenPGP

File Encryption

```
C:\WINDOWS\system32\cmd.exe

C:\>gpg -o Vertrag.pdf -d Vertrag.pdf.gpg
gpg: detected reader 'Gemplus USB Smart Card Reader 0'
gpg: detected reader 'Texas Instruments SmartCardSlot 0'

Please enter the PIN
gpg: encrypted with 1024-bit RSA key, ID B6714A62, created 2010-02-23
      "Hans Mustermann <test@example.com>"
File 'Vertrag.pdf' exists. Overwrite? (y/N) y
gpg: Signature made 02/23/10 23:58:10 using RSA key ID F1D596B1
gpg: Good signature from "Hans Mustermann <test@example.com>"
```



User Authentication in the Web

The screenshot shows a web browser window at <http://webid.fcns.eu/>. The page displays a 'MyProfile' section with a 'Welcome!' message and a list of actions: 'Login with your WebID', 'Lookup a WebID profile', 'Generate a WebID certificate', 'Generate a local WebID profile', 'Register your WebID', and 'Convert a WebID profile into RDF/JSON'. A 'User Identification Request' dialog box is overlaid on the page. The dialog box contains the following text:

User Identification Request

This site has requested that you identify yourself with a certificate:
*.fcns.eu (:443)
Organization: "*.fcns.eu"
Issued Under: "Alpha"

Choose a certificate to present as identification:

CryptoStick C7F:CAcert WoT User [0A:5C:65]

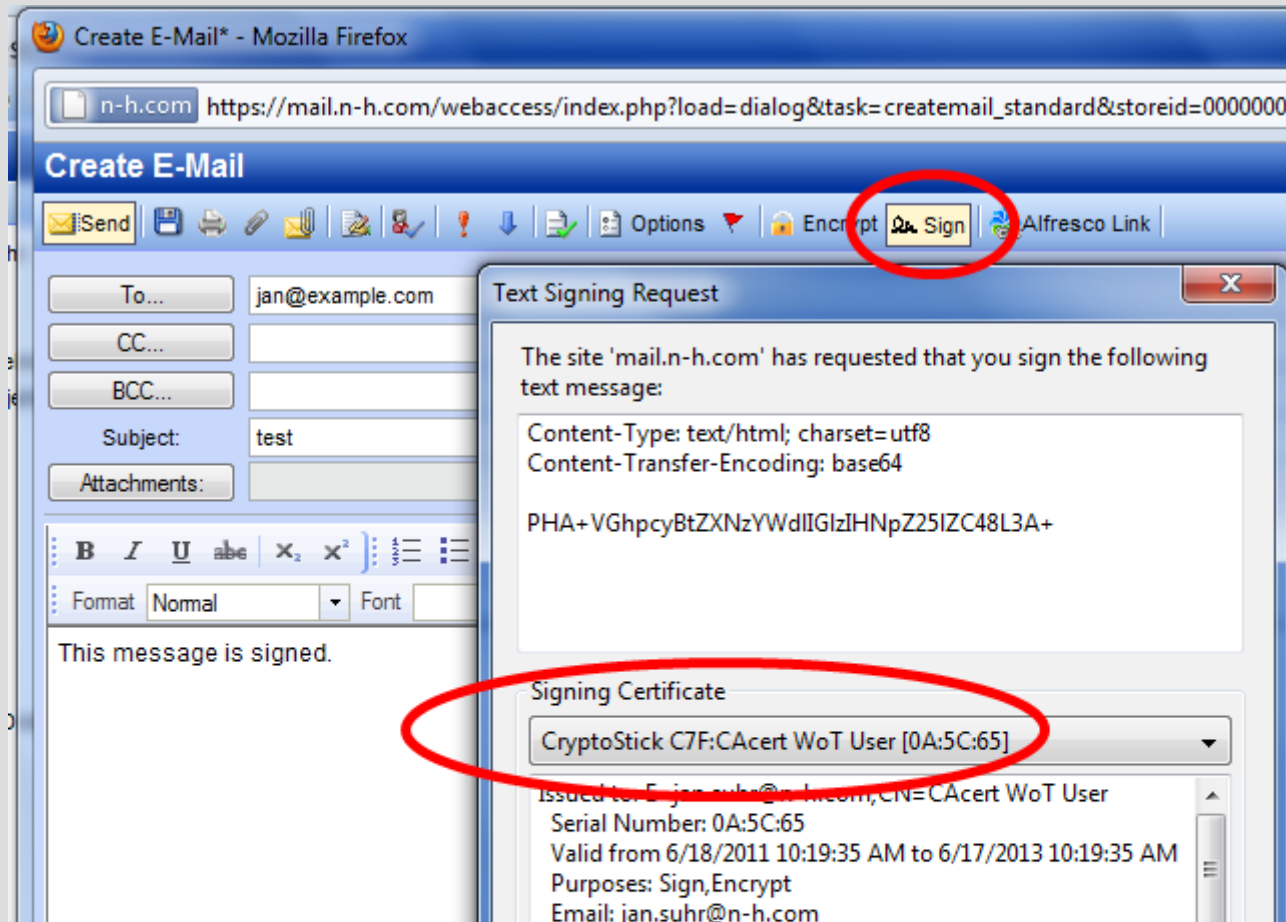
Details of selected certificate:

Issued to: E=jan.suhr@n-h.com,CN=CAcert WoT User
Serial Number: 0A:5C:65
Valid from 6/18/2011 10:19:35 AM to 6/17/2013 10:19:35 AM
Purposes: Sign,Encrypt
Email: jan.suhr@n-h.com
Issued by: E=support@cacert.org,CN=CA Cert Signing Authority,OU=http://www.cacert.org,O=Root CA
Stored in: CryptoStick C7F

Remember this decision

OK Cancel

Zarafa – Signing of Emails



Next Version 2

- HTML interface
- Encrypted storage
- Broad software support
- Metal case



Organization

- German Privacy Foundation e.V.
- Production is non-profit
- Open community – get involved!



GERMAN
PRIVACY
FOUNDATION e.V.

German Privacy Foundation e.V. (GPF)

- Anonymization services:
 - Tor Partner program
 - Jondonym (JAP)
 - I2P
- Uncensored DNS
- Privacy Box
- Privacy Handbuch
- Trainings
- ...



GERMAN
PRIVACY
FOUNDATION e.V.

Availability of the Crypto Stick



non-profit price: 49 € !

<https://www.privacyfoundation.de/shop/>



GERMAN
PRIVACY
FOUNDATION e.V.



**GERMAN
PRIVACY
FOUNDATION e.V.**

1.7.2011, Jan Suhr