GERMAN PRIVACY FOUNDATION e.V.

1.7.2011, Jan Suhr

Problem:
Do You Trust Your Internet Cafe?

AP / Greg Baker

Problem: Do You Trust Your Internet Service Provider?

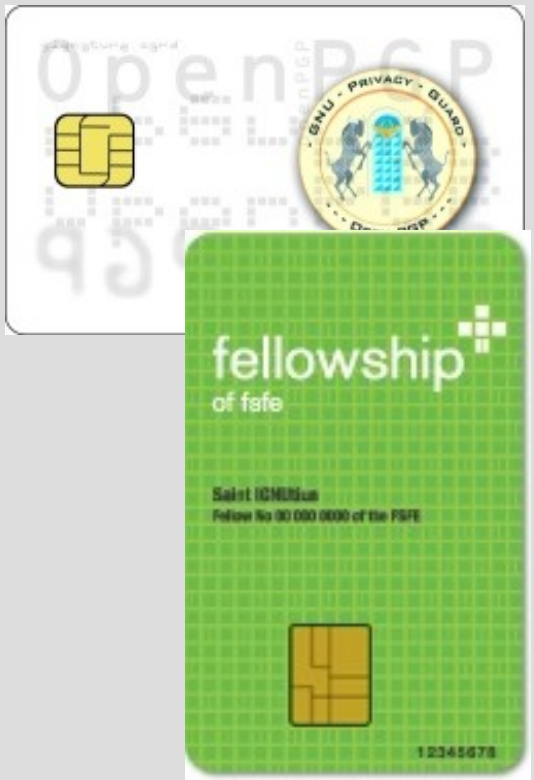
Intercept your e-mails, chat, social websites → Encryption e.g. GnuPG

Track your web surfing
Censor the Internet → Tor, Jondonym

GERMAN PRIVACY FOUNDATION e.V.

Solution: Security Token

OpenPGP Card v2



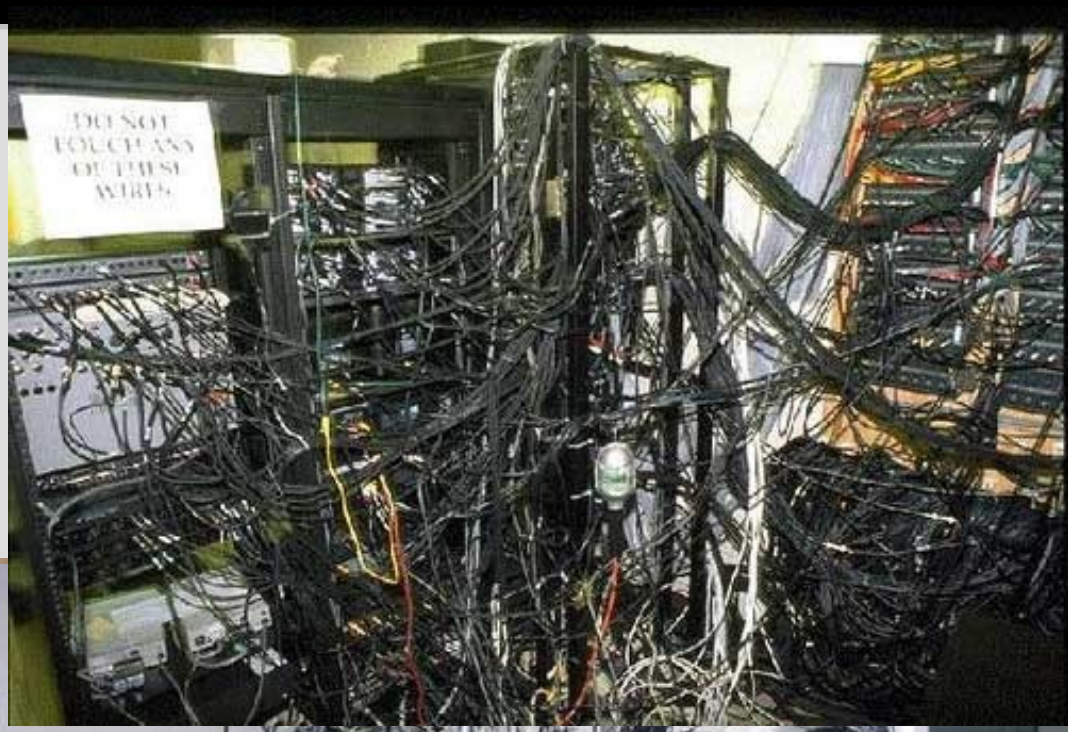
+

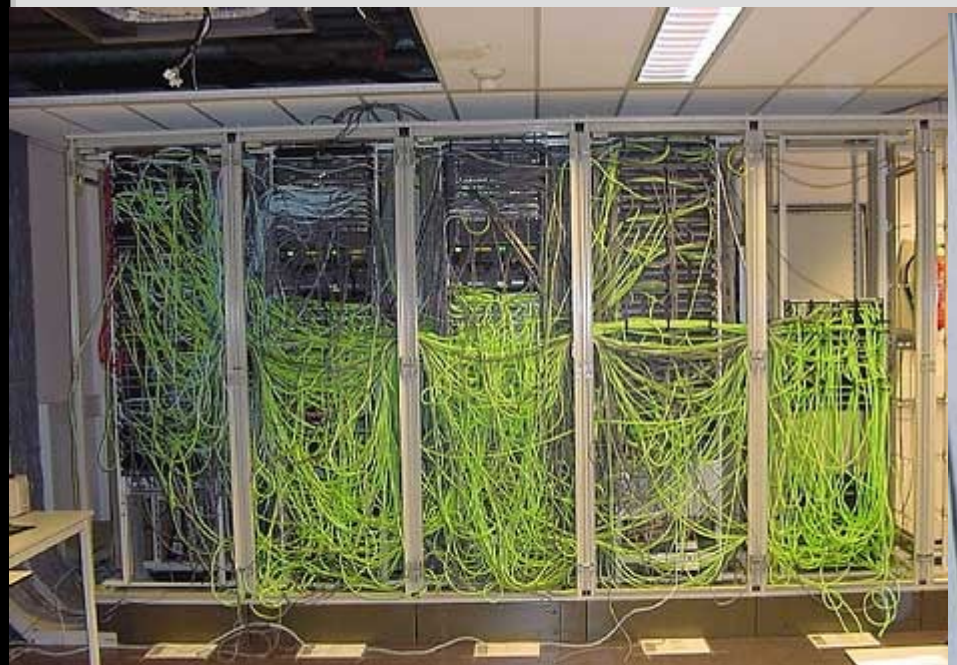
Smartcard adapter

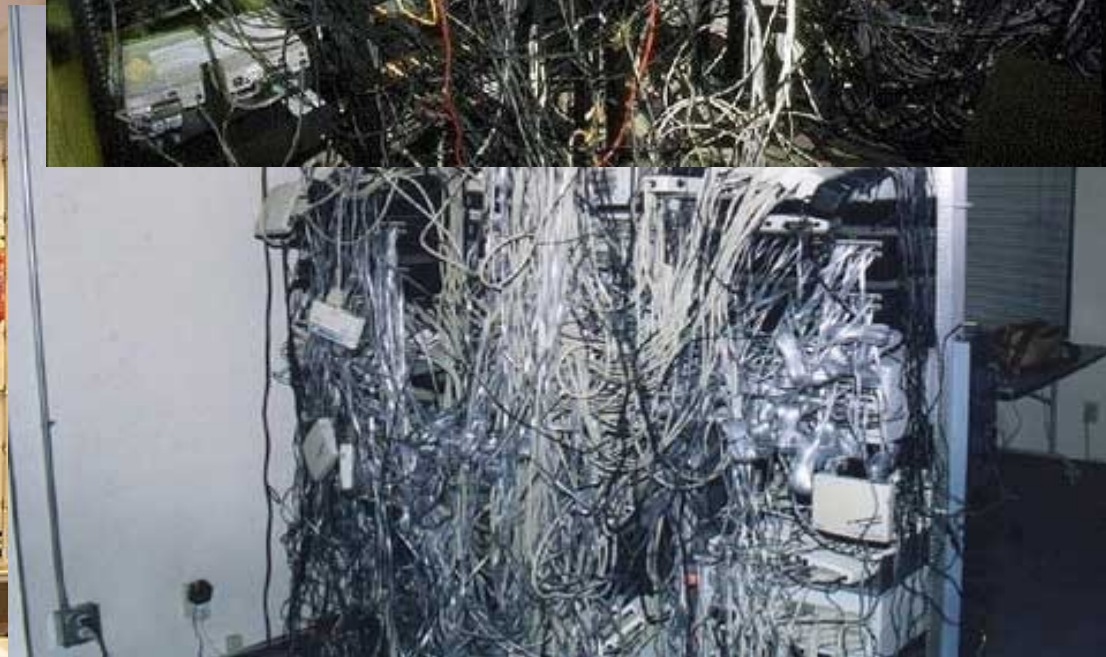
GERMAN PRIVACY FOUNDATION e.V.

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

GERMAN PRIVACY FOUNDATION e.V.

Features

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

GERMAN PRIVACY FOUNDATION e.V.

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

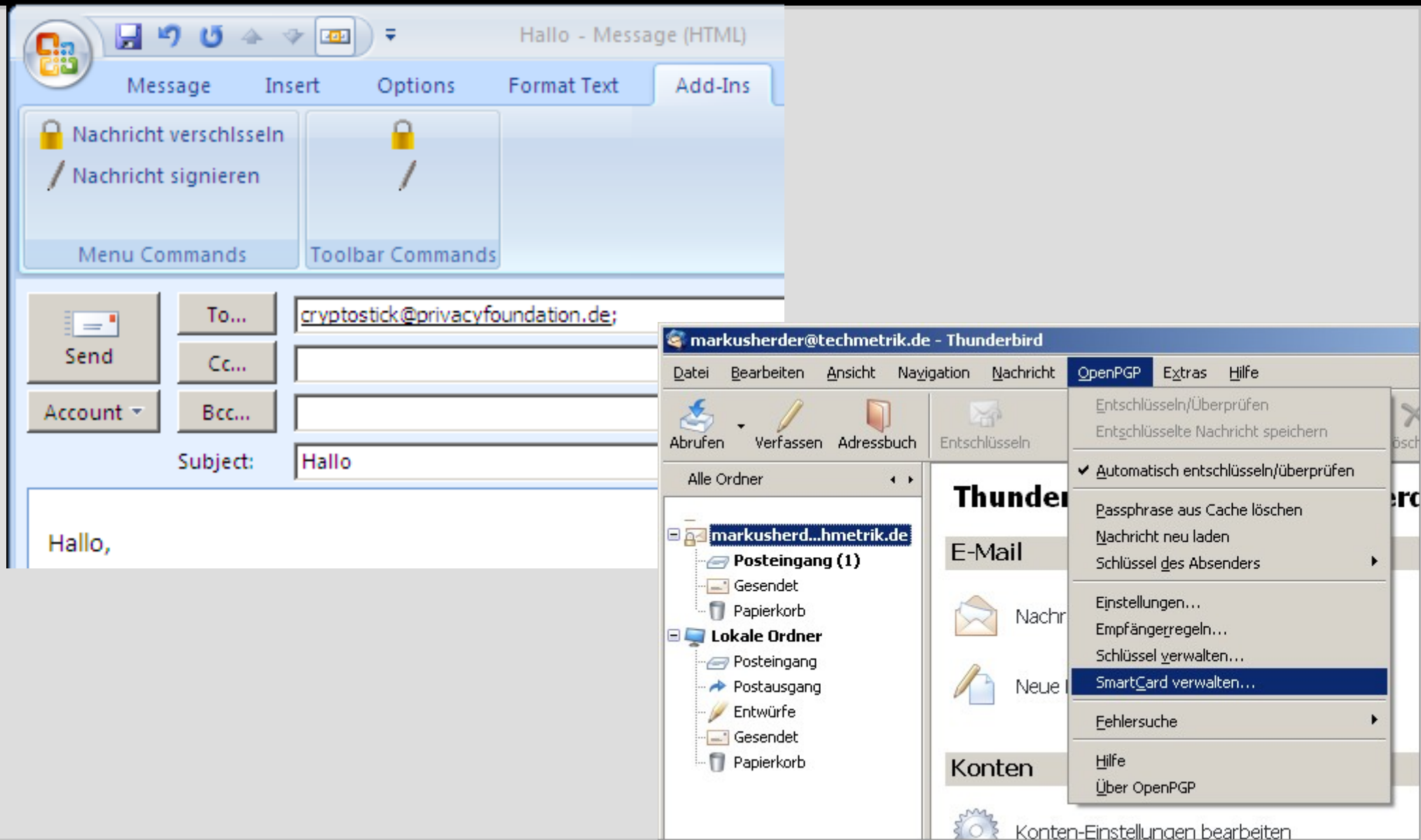
GERMAN PRIVACY FOUNDATION e.V.

Compatible Applications

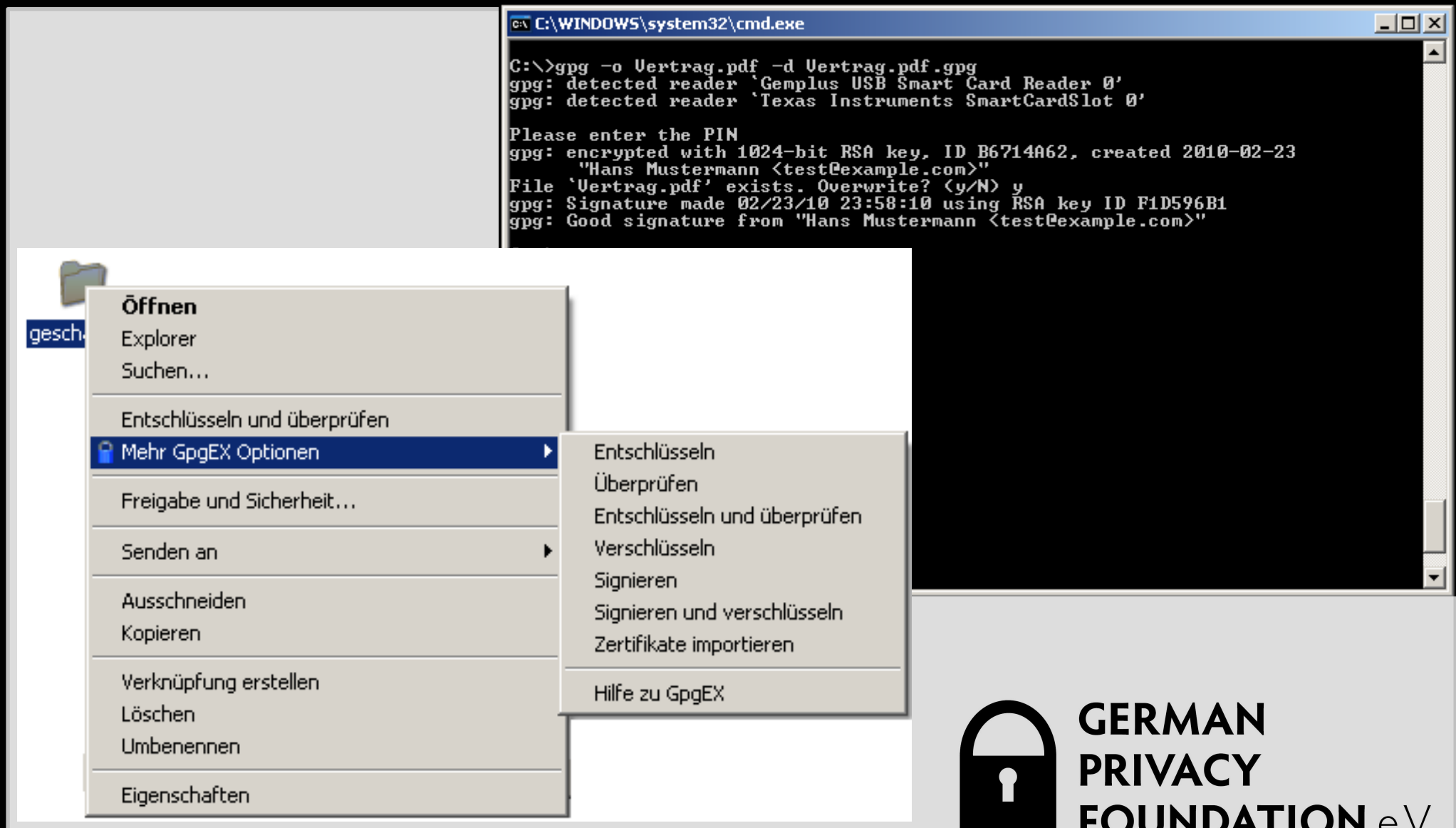
- Linux, Windows, Mac OS
- GnuPG, Thunderbird+Enigmail, Evolution, MS Outlook
- SSH, OpenVPN
- Linux authentification
- TrueCrypt, Thunderbird, Firefox, PKCS#11 compliant

GERMAN PRIVACY FOUNDATION e.V.

Email Encryption

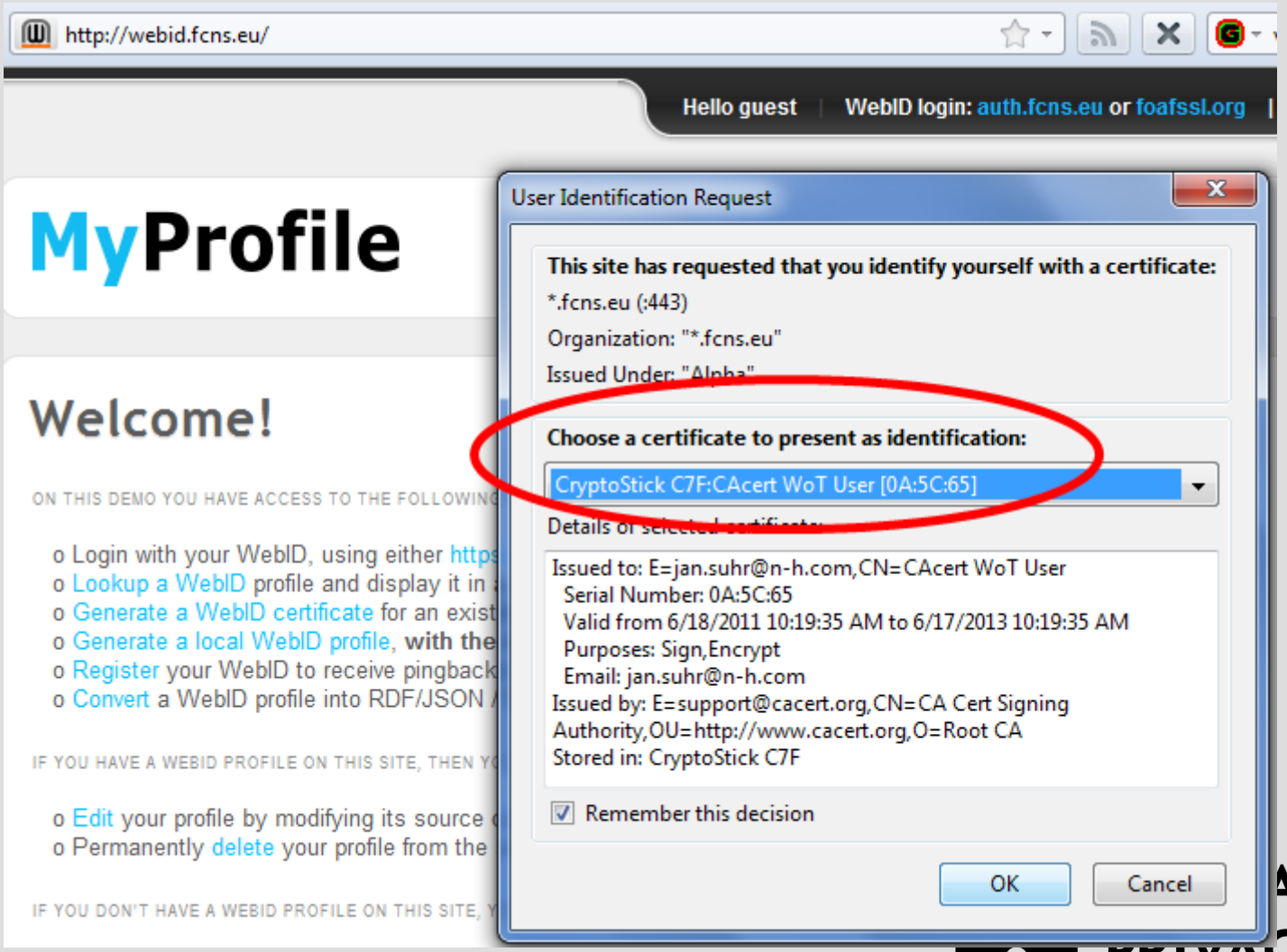


File Encryption



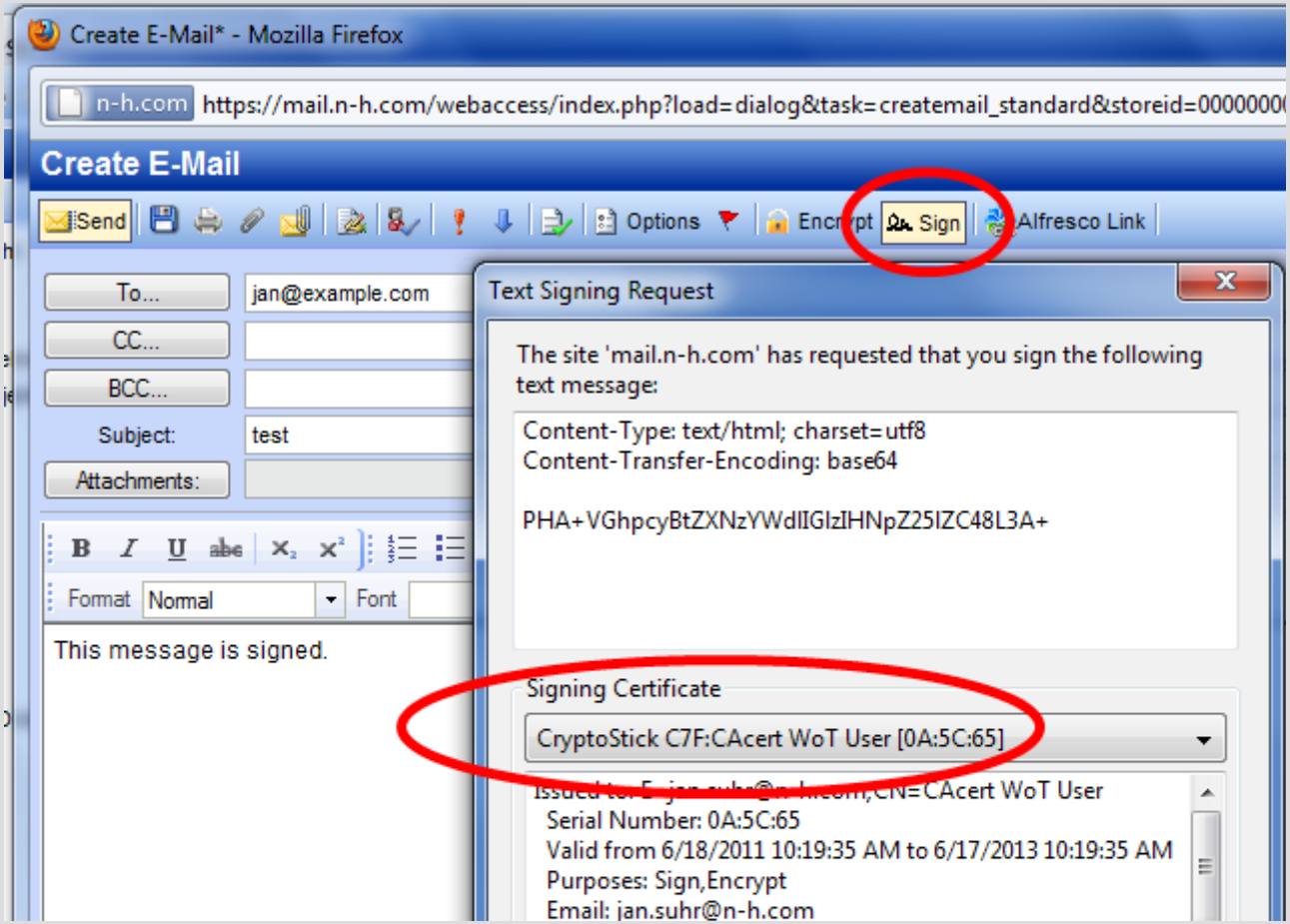
GERMAN PRIVACY FOUNDATION e.V.

User Authentication in the Web



AN PRIVACY FOUNDATION e.V.

Zarafa – Signing of Emails



GERMAN PRIVACY FOUNDATION e.V.

Next Version 2

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

GERMAN
PRIVACY
FOUNDATION e.V.

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