Praktische eMail-Verschüsselung

Linux Café im BIZ Nürnberg

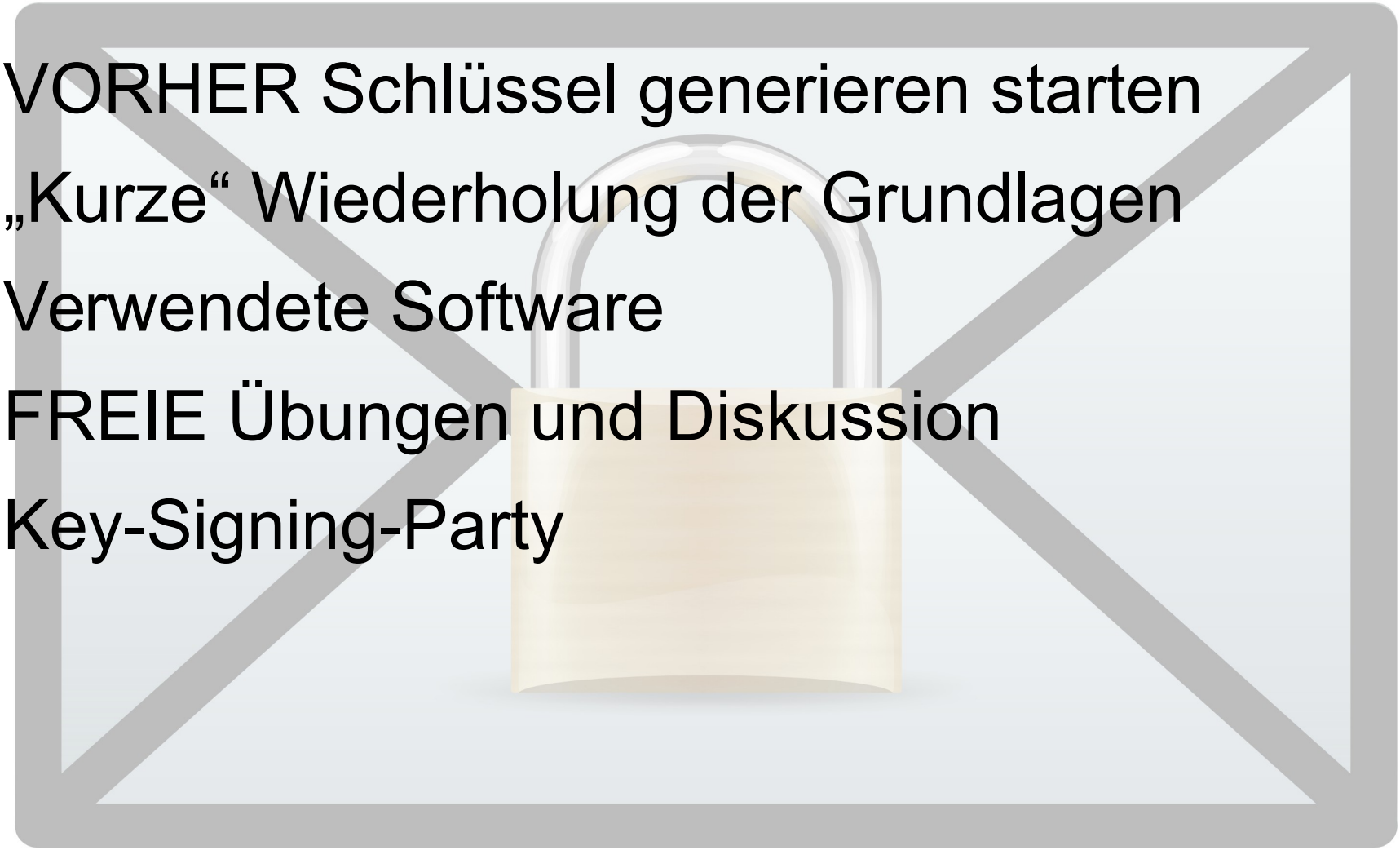
Raum 4.18

Arno Zeitler (info@amtuxtisch.de)

8.6.2015

Rechtliches

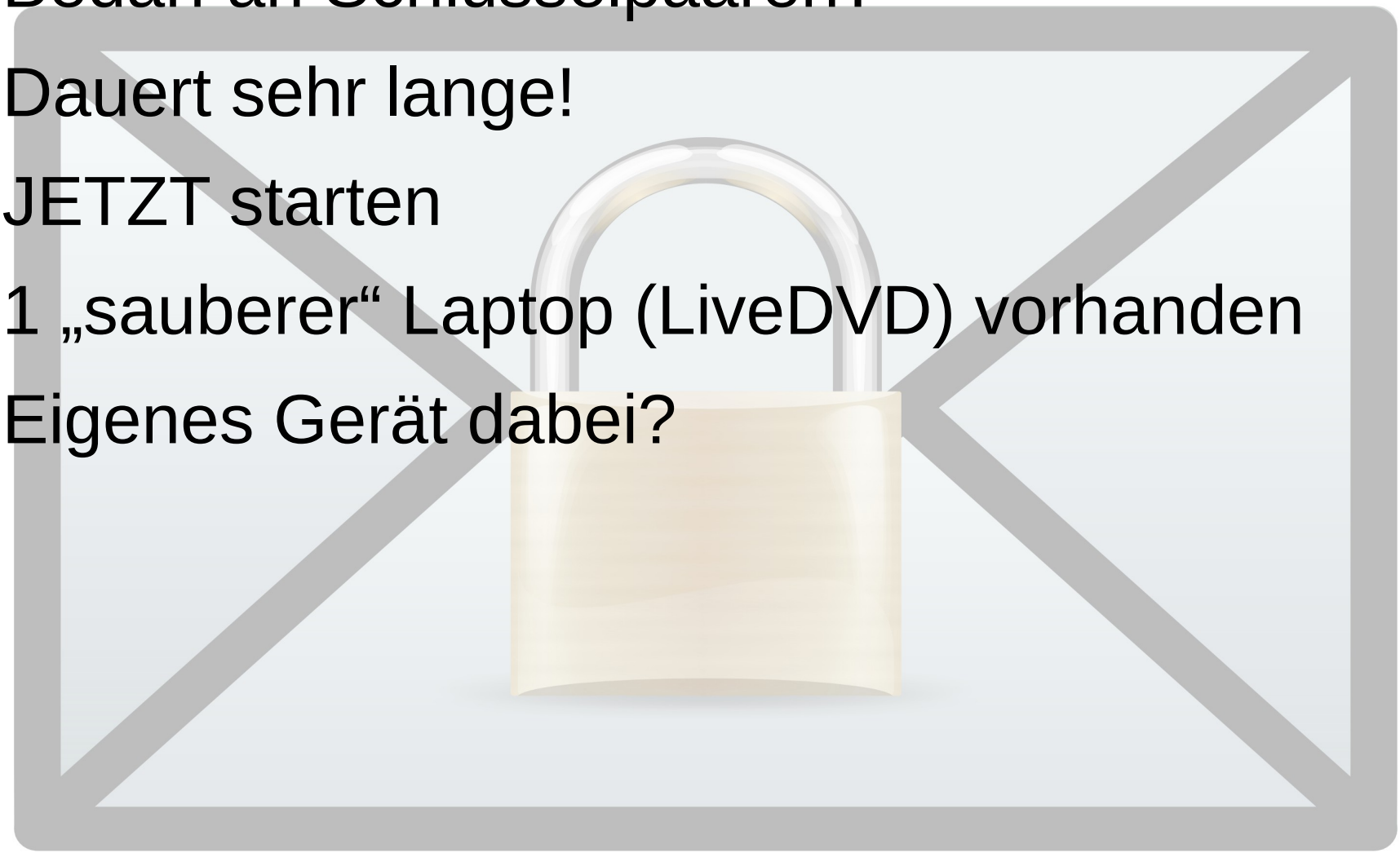
Heute Abend



- VORHER Schlüssel generieren starten
- „Kurze“ Wiederholung der Grundlagen
- Verwendete Software
- FREIE Übungen und Diskussion
- Key-Signing-Party

Schlüssel generieren starten

- Bedarf an Schlüsselpaaren?
- Dauert sehr lange!
- JETZT starten
- 1 „sauberer“ Laptop (LiveDVD) vorhanden
- Eigenes Gerät dabei?



Grundlagen - Motivation

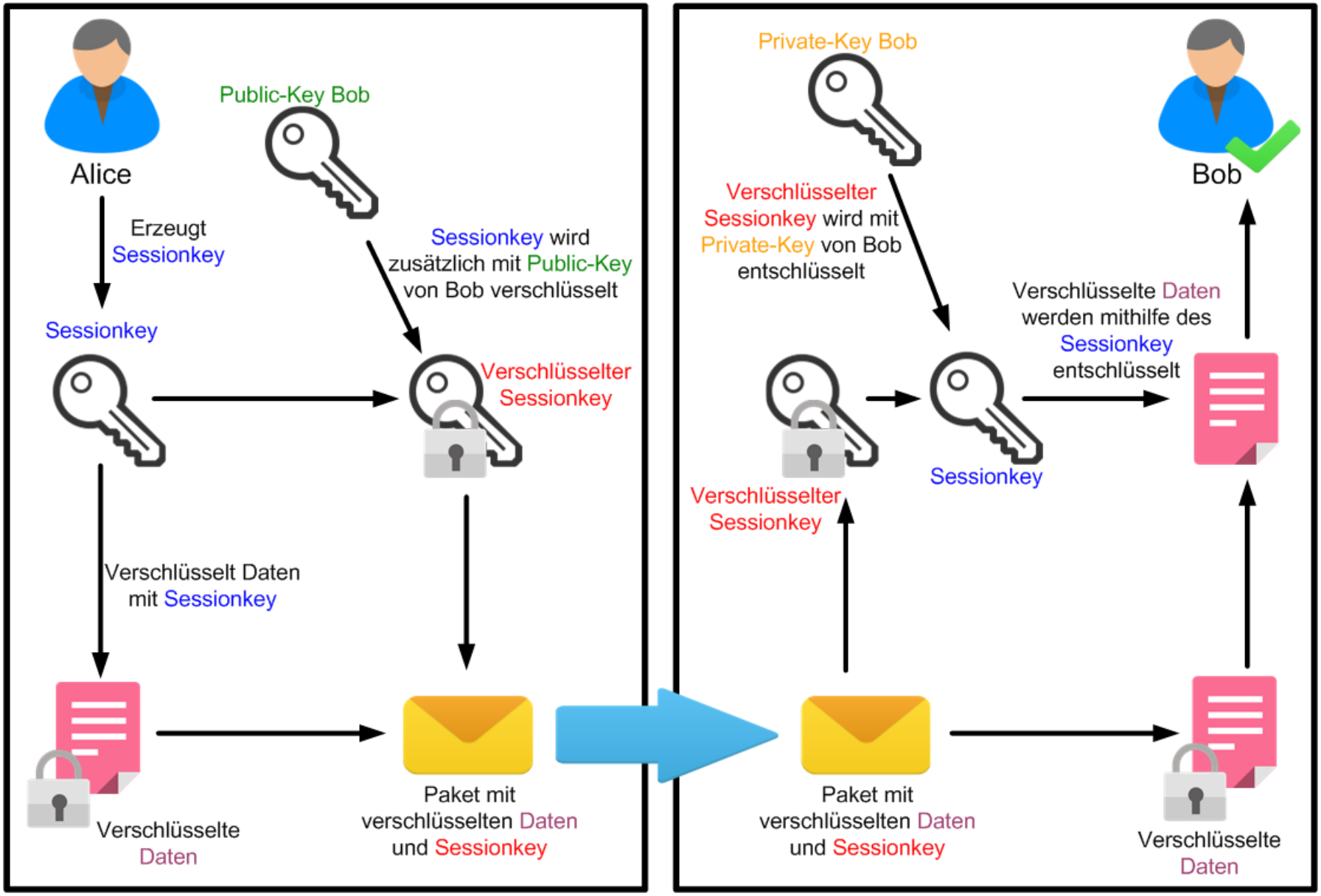
- Wahrung der Privatsphäre
- Schutz von Informationen gegen
  - Ausspähen → Verschlüsselung(Autorisierung)
  - Sabotage → Signatur(Authentizität/Integrität)
- Erschweren der Massenüberwachung
  - “So viele eMail wie möglich verschlüsseln!”
  - Achtung UNgeschützt: Wer Wann Was mit Wem!

„Privatsphäre ist ein Recht wie jedes andere. Man muss es in Anspruch nehmen, oder man riskiert es zu verlieren.” Phil Zimmermann

Grundlagen – techn. Details

- Client-basierte Verschlüsselung
- Lokale Schlüsselbunde (~/.gnupg/-Dateien)
- Asymmetrische Schlüsselpaare
  - Sehr große Zahlen math. untrennbar verknüpft
  - Privat NUR unterschreiben / entschlüsseln
  - Öffentlich NUR verschlüsseln / Unterschrift prüfen
- Web of Trust (ggs. unterschreiben öffentl. Schlüssel)
- Schlüssel-Server (öffentl. Schlüssel / Replikate weltw.)
- Hybride Verschlüsselung (Zufalls-Sitzungsschlüssel)
  - asymmetrische Schlüsselübertragung
  - symmetrisch verschlüsselte Datenübertragung

Grundlagen – Ablauf



Quelle: http://commons.wikimedia.org/wiki/User:Dekocrypt

Grundlagen – WOT I

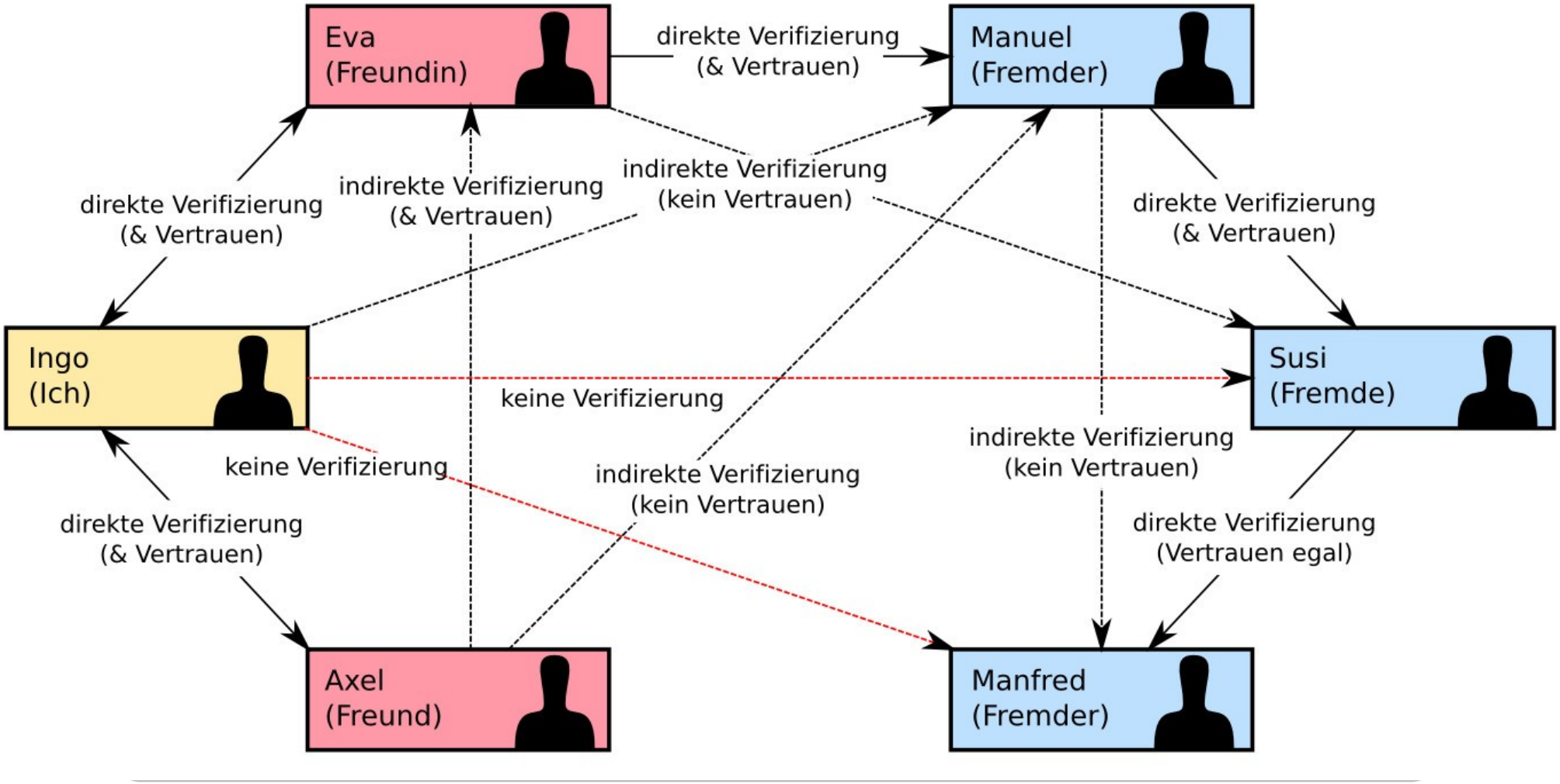
- WOT – das Web Of Trust
- Auch Website-Bewertungsplattform – hier nicht!
- Alternative zu hierarchischen PKI-Systemen
- Vorsicht: Jeder kann behaupten Person zu sein!
- Gegenseitiges unterschreiben öffentl. Schlüssel
  - Mit privaten Schlüsseln
  - Möglichst genaue Prüfung Schlüssel / Person
- Verteilung via Schlüsselservern mit Replikation
- Gesteuert via lokal wirkendes Besitzervertrauen
- Mindestens ein absolutes Vertrauen erforderlich

Grundlagen – WOT II

- Vertrauen gegenüber dem Schlüsselinhaber
  - Seine korrekte Identität
  - Seine korrekte Prüfung der Identität Anderer
- Datenschutzprobleme
  - Jeder kann öffentliche Schlüssel signieren und auf Schlüsselserver hochladen
  - Identitäten und die Liste derer die die Identität geprüft haben sind öffentlich
  - Soziale Netzwerke maschinell lesbar
  - Schlüssel können nie mehr gelöscht werden
  - Ausweg: Neues Schlüsselpaar (Neubeginn)

Grundlagen – WOT

- WOT – das Web Of Trust



Quelle: https://commons.wikimedia.org/wiki/User:Ogmios

Verwendete Software – Versionen

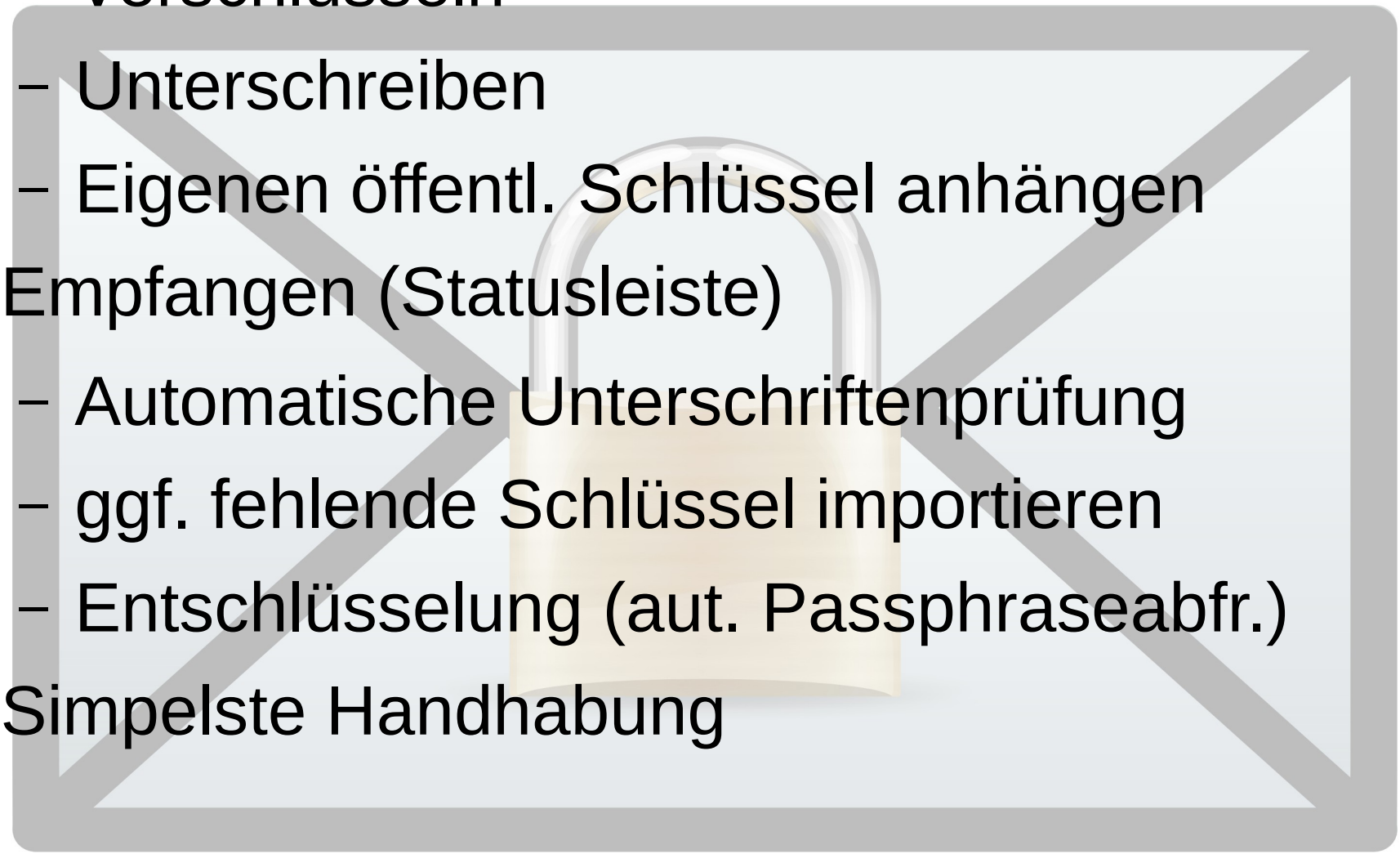
- GnuPG
  - Ubuntu 14.04.2 LTS = 1.4.16
  - Upgrade auf GnuPG2 (!) 2.0.22 erst mit nächster Enigmail Version notwendig!
  - Unterschiedliche .deb → installieren
- Thunderbird (derzeit 31.7.0)
- Enigmail-Plugin für Thunderbird
  - Ubuntu Repository veraltet / keine Updates
  - Thunderbird → Exras → Add-ons V 1.8.2
- Seahorse 3.10.2 Schlüsselverwaltung
- ACHTUNG: ältere Versionen → Sicherheitsfehler!

Funktionen – Schlüssel

- Erzeugen (Schlüsselpaare, Widerrufszert.)
- Anzeigen (private, öffentliche, „gefiltert“)
  - Schlüsseleigenschaften (Fingerabdruck, ID)
  - Unterschriften
- Importieren / Exportieren
- Schlüsselserver (suchen, hochladen, aktualis.)
- Unterschreiben (öffentlich)
- Besitzervertrauen festlegen (lokal)
- Parameter ändern (Benutzerkennungen, Ablaufdatum, Passphrase, Foto, Empfängerr...)

Funktionen – eMails benutzen

- Verfassen (Bedien- / Statusleiste Enigmail)
  - Verschlüsseln
  - Unterschreiben
  - Eigenen öffentl. Schlüssel anhängen
- Empfangen (Statusleiste)
  - Automatische Unterschriftenprüfung
  - ggf. fehlende Schlüssel importieren
  - Entschlüsselung (aut. Passphraseabfr.)
- Simpelste Handhabung



Übungen I

- Arbeitsplätze von 01 bis 12 für XX
  - Adresse: enigmaXX.biz@gmx.de
  - Passphrase: EnigmaXX.Geheimnis
- Konfiguration im 'terminal' vorbereiten
  - `'mv .thunderbird .thunderbird.orig'`
  - `'mv .gnupg .gnupg.orig'`
  - `'tar -xvpzf enigmaXX*.tgz'`
- edward-de@fsf.org (https://emailselfdefense.fsf.org/de/ Schritt 3)
  - öffentl. Schlüssel unverschlüsselt senden
  - Edwards Antwort verschlüsselt beantworten
  - Edwards Schlüssel vom Server holen ...

Übungen II

- EnigmaXX's öffentlichen Schlüssel auf Server
- Fingerabdruck gegenchecken
- „SitzNachbarn” eMails schreiben
  - Verschlüsselt
  - Unterschrieben
  - An mehrere Empfänger
- Schüssel gegenseitig signieren
- Unterschiede beobachten (unsig. / sig. / n-sig.)
- Eigene Ideen einbringen ...

„Key-Signing-Party“

- Rechner Vertrauenswürdig?! (LiveDVD!)
- Echtheit der Person → Ausweisdokument!
- Öffentlichen Schlüssel identifizieren
- Eineindeutig nur via Fingerabdruck!
- eMail an Schlüsselinhaber → soll Inh. sagen
- Schlüssel unterschreiben
  - von Schlüsselserver laden
  - Unterschreiben
  - auf Schlüsselserver hoch laden
- ... in die Welt tragen und praktizieren!

Referenzen

Links:

https://emailselfdefense.fsf.org/de/

https://www.gnupg.org/

https://www.mozilla.org/de/thunderbird/

https://www.enigmail.net/

https://www.thunderbird-mail.de/wiki/Enigmail_OpenPGP

http://www.pgpi.org/

http://www.selbstdatenschutz.info/e-mail_verschluesseln

http://de.wikipedia.org/ verschiedene

http://www.bfdi.bund.de/DE/Home/home_node.html