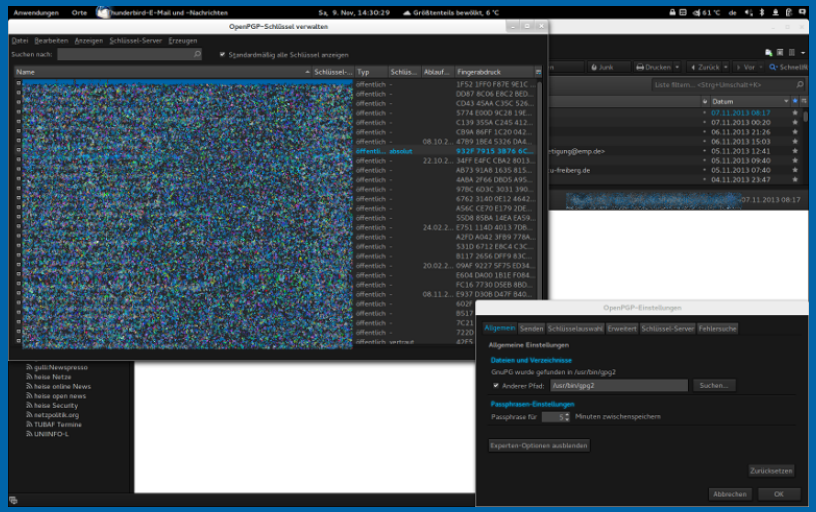
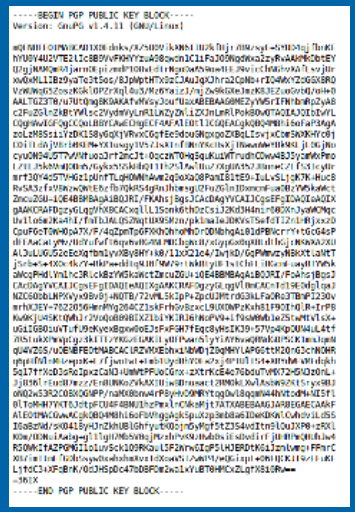
TECHNISCHE UNIVERSITÄT
BERGAKADEMIE FREIBERG
Die Ressourcenuniversität. Seit 1765.

E-Mail-Verschlüsselung via GnuPG

mit Thunderbird und Enigmail oder Evolution und Seahorse





Klickpfade für alle im Vortrag an der Software demonstrierten Schritte

Teil 1:
GnuPG mit Thunderbird und Enigmail

WORUM ES HEUTE GEHT

- benötigte Software
- Installation & Einrichtung
- Durchlauf des Assistenten von Enigmail
- eigenes (zusätzliches) Schlüsselpaar manuell anlegen
- eigenen öffentlichen Schlüssel auf einen Keyserver hochladen
- eigenen öffentlichen Schlüssel in eine Datei exportieren
- eigenen Schlüssel deaktivieren und/oder zurückziehen
- Schlüssel von Kommunikationspartnern importieren
- Besitzervertrauen festlegen
- überprüfte Schlüssel signieren und neu hochladen
- Schlüssel von Kommunikationspartnern löschen
- verschlüsselte und/oder signierte Mails versenden

BENÖTIGTE SOFTWARE

- **Thunderbird** – E-Mail Client
- **GnuPG** – Programm zum Ver- und Entschlüsseln der Nachrichten sowie zur Verwaltung der Schlüssel (CLI)
- **Enigmail** – Add-On für Thunderbird, welches eine grafische Schnittstelle für GnuPG bietet

INSTALLATION (DEBIAN-DERIVATE)

- Terminal:
  `sudo apt-get install thunderbird thunderbird-enigmail`
  Debian: Thunderbird → Icedove
- oder: Enigmail über die Add-On-Verwaltung von TB installieren:
  TB → Extras → Add-Ons → Add-Ons suchen → Suche nach Enigmail → Button „Installieren“
- gnupg 1.4 ist oft standardmäßig installiert (Paketverwaltung), sonst:
  `sudo apt-get install gnupg`
- falls gewünscht: `sudo apt-get install gnupg2`
  Nachträglicher Wechsel von gnupg auf gnupg2 unter beibehalten des Schlüsselbundes ist jederzeit möglich (V2 beherrscht S/MIME).

EINRICHTUNG

- Konten in TB einrichten: TB → Assistent startet beim ersten Start von TB automatisch und ist selbsterklärend, sonst unter TB → Bearbeiten → Konten-Einstellungen → Konten-Aktionen → E-Mail-Konto hinzufügen ein neues Konto einrichten
- überprüfen, ob der Pfad zur Binary stimmt:
  TB → OpenPGP → Einstellungen → Allgemein
  Der Pfad sollte `/usr/bin/gpg` bzw. `/usr/bin/gpg2` lauten; er lässt sich im Vorfeld mit `which gpg` bzw. `which gpg2` im Terminal ermitteln.
- Empfehlung: zusätzliches Verschlüsseln mit eigenem Schlüssel aktivieren, sonst landen unlesbare Nachrichten im Postausgang:
  TB → OpenPGP → Einstellungen → Senden → Häkchen setzen
- optional: weitere Keyserver hinzufügen, z.B. keyserver.ubuntu.com:
  TB → OpenPGP → Einstellungen → Schlüssel-Server

DURCHLAUF DES ASSISTENTEN VON ENIGMAIL

- TB → OpenPGP → OpenPGP-Assistent selbsterklärend, richtet Verschlüsselung in den Kontoeinstellungen für die gewünschte(n) Adresse(n) ein und erstellt eigenes Schlüsselpaar
- Wichtig: gute PassPHRASE wählen und Widerrufszertifikat anlegen!

EIGENES (ZUSÄTZLICHES) SCHLÜSSELPAAR MANUELL ANLEGEN

- TB $\rightarrow$ OpenPGP $\rightarrow$ Schlüssel verwalten $\rightarrow$ Erzeugen $\rightarrow$ neues Schlüsselpaar
- Wichtig: gute PassPHRASE wählen und Widerrufszertifikat anlegen!

EIGENEN ÖFFENTLICHEN SCHLÜSSEL HOCHLADEN

- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf eigenen Schlüssel → auf Schlüsselserver hochladen → Server wählen → OK

EIGENEN ÖFFENTLICHEN SCHLÜSSEL IN EINE DATEI EXPORTIEREN

- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf eigenen Schlüssel → in Datei exportieren → öffentlichen Schlüssel wählen → Speicherort wählen → Speichern
- Auch der eigene geheime Schlüssel und die öffentlichen Schlüssel von Kommunikationspartnern können für ein Backup exportiert werden.

EIGENEN SCHLÜSSEL DEAKTIVIEREN UND/ODER ZURÜCKZIEHEN

- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf eigenen Schlüssel → Deaktivieren (reversibel)
- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf eigenen Schlüssel → Zurückziehen (irreversibel)
- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf eigenen Schlüssel → Auf Schlüsselserver hochladen → Server wählen → OK

SCHLÜSSEL VON KOMMUNIKATIONSPARTNERN IMPORTIEREN

- von Servern bei signierten E-Mails im Posteingang:
  TB → Posteingang → signierte E-Mail → Details → Schlüssel importieren → Importieren → Keyserver wählen → OK
- von Servern über die Suche nach IDs:
  TB → OpenPGP → Schlüssel verwalten → Schlüssel-Server → Schlüssel suchen → Keyserver wählen → Nutzer-ID (E-Mail-Adresse) oder Schlüssel-ID eingeben → OK
- Schlüssel für alle gespeicherten Kontakte suchen:
  TB → OpenPGP → Schlüssel verwalten → Schlüssel-Server → Schlüssel für alle Kontakte suchen → Fortsetzen
  Achtung: kann sehr lange dauern! → Kaffee kochen

SCHLÜSSEL VON KOMMUNIKATIONSPARTNERN IMPORTIEREN II

- aus einer Datei:
  TB → OpenPGP → Schlüssel verwalten → Datei → Importieren → Datei wählen → OK
- aus der Zwischenablage:
  Schlüsselblock markieren → Strg+C → TB → OpenPGP → Schlüssel verwalten → Bearbeiten → Aus Zwischenablage importieren → Importieren

SCHLÜSSELVERTRAUEN

- Fingerprint überprüfen:
  TB → OpenPGP → Schlüssel verwalten →
  Rechtsklick auf betreffenden Schlüssel →
  Schlüsseleigenschaften → Fingerabdruck
- Unterschriften überprüfen:
  TB → OpenPGP → Schlüssel verwalten →
  Rechtsklick auf betreffenden Schlüssel →
  Unterschriften anzeigen → nach Unterschriften von Schlüsseln mit hohem Besitzervertrauen suchen

ÜBERPRÜFTE SCHLÜSSEL SIGNIEREN UND NEU HOCHLADEN

Zuerst von der Korrektheit des Schlüssels und der Zuordnung zur betreffenden Person überzeugen!

- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf betreffenden Schlüssel → Unterschreiben → persönlichen Schlüssel wählen, falls mehrere vorhanden → Grad der Überprüfung festlegen → OK
- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf betreffenden Schlüssel → Auf Schlüsselserver hochladen → Server wählen → OK

BESITZERVERTRAUEN FESTLEGEN

- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf betreffenden Schlüssel → Besitzervertrauen festlegen → Vertrauensstufe wählen → OK

Dabei gilt:

- frisch importierte Schlüssel haben immer Stufe unbekannt
- Stufe absolut nur für eigene Schlüssel
- Stufe voll für Personen, zu denen man auch im realen Leben volles Vertrauen hat, deren Schlüssel man überprüft hat und die dafür bekannt sind, sorgsam mit Schlüsseln umzugehen, insbesondere auch beim Signieren fremder Schlüssel.
- Stufe wenig für Personen, die man kennt und deren Schlüssel man überprüft hat
- Stufe unbekannt behalten, wenn man keine Aussage treffen kann
- Stufe NICHT für alle anderen

SCHLÜSSEL VON KOMMUNIKATIONSPARTNERN LÖSCHEN

- TB → OpenPGP → Schlüssel verwalten → Rechtsklick auf betreffenden Schlüssel → Löschen → Löschen

VERSCHLÜSSELTE UND/ODER SIGNIERTE E-MAILS VERSENDEN

- Auf verschlüsselte/unterschriebene E-Mails wird standardmäßig verschlüsselt/unterschrieben geantwortet.
- TB $\rightarrow$ Verfassen $\rightarrow$ OpenPGP $\rightarrow$ Nachricht unterschreiben/verschlüsseln oder Buttons unten rechts in der neuen Nachricht

Teil 2:
GnuPG mit Evolution und Seahorse

WORUM ES HEUTE GEHT

- benötigte Software
- Installation & Einrichtung
- eigenes Schlüsselpaar anlegen
- eigenen öffentlichen Schlüssel auf einen Keyserver hochladen
- eigenen öffentlichen Schlüssel in eine Datei exportieren
- eigenen Schlüssel zurückziehen
- Schlüssel von Kommunikationspartnern importieren
- Besitzervertrauen festlegen
- überprüfte Schlüssel signieren und neu hochladen
- Schlüssel von Kommunikationspartnern löschen
- verschlüsselte und/oder signierte Mails versenden

BENÖTIGTE SOFTWARE

- **Evolution** – E-Mail Client
- **GnuPG** – Programm zum Ver- und Entschlüsseln der Nachrichten sowie zur Verwaltung der Schlüssel (CLI)
- **Seahorse** – Software zum Verwalten von Schlüsseln und Passwörtern (grafisch)

INSTALLATION (DEBIAN-DERIVATE)

- Terminal:
  `sudo apt-get install evolution seahorse`
  Bei Ubuntu ist Seahorse standardmäßig installiert („Passwörter und Verschlüsselung“).
- gnupg 1.4 ist oft standardmäßig installiert (Paketverwaltung), sonst:
  `sudo apt-get install gnupg`
- falls gewünscht: `sudo apt-get install gnupg2`
  Nachträglicher Wechsel von gnupg auf gnupg2 unter beibehalten des Schlüsselbundes ist jederzeit möglich (V2 beherrscht S/MIME).

EIGENES SCHLÜSSELPAAR ANLEGEN

- Seahorse → Datei → Neu → PGP-Schlüssel → weiter
- Wichtig: gute PassPHRASE wählen!
- optional: weitere Keyserver hinzufügen: Seahorse → Bearbeiten → Einstellungen → Hinzufügen

EIGENEN ÖFFENTLICHEN SCHLÜSSEL HOCHLADEN

- Seahorse → GnuPG-Schlüssel → eigenen Schlüssel markieren → Entfernt → Schlüssel abgleichen und veröffentlichen → Abgleichen
- Es wird der Keyserver verwendet, der unter Bearbeiten → Einstellungen → Schlüssel veröffentlichen gewählt ist.

EIGENEN ÖFFENTLICHEN SCHLÜSSEL IN EINE DATEI EXPORTIEREN

- Öffentlichen Schlüssel für Weitergabe: Seahorse → GnuPG-Schlüssel → eigenen Schlüssel markieren → Datei → Exportieren → als Dateityp „E-Mail-sichere PGP-Schlüssel“ wählen → Speicherort wählen → Exportieren
- Gesamten Schlüssel für Backup: Seahorse → GnuPG-Schlüssel → Rechtsklick auf eigenen Schlüssel → Eigenschaften → Reiter „Details“ → Exportieren

EIGENEN SCHLÜSSEL ZURÜCKZIEHEN

- Seahorse → GnuPG-Schlüssel → Rechtsklick auf eigenen Schlüssel → Eigenschaften → Reiter „Details“ → Unterschlüssel markieren → Widerrufen
- Seahorse → GnuPG-Schlüssel → eigenen Schlüssel markieren → Entfernt → Schlüssel abgleichen und veröffentlichen → Abgleichen

SCHLÜSSEL VON KOMMUNIKATIONSPARTNERN IMPORTIEREN

- Aus einer Datei:
  Seahorse → Datei → Importieren → Datei auswählen → Öffnen
- Vom Keyserver:
  Seahorse → Entfernt → Entfernte Schlüssel suchen

SCHLÜSSELVERTRAUEN

- Fingerprint überprüfen:
  Seahorse → GnuPG-Schlüssel → Rechtsklick auf betrefenden Schlüssel → Eigenschaften → Reiter „Details“ → Fingerabdruck
- Unterschriften überprüfen:
  Seahorse → GnuPG-Schlüssel → Rechtsklick auf betrefenden Schlüssel → Eigenschaften → Reiter „Vertrauen“ → unter „Personen die diesen Schlüssel signiert haben“ nach Unterschriften von Schlüsseln mit hohem Besitzervertrauen suchen

ÜBERPRÜFTE SCHLÜSSEL SIGNIEREN UND NEU HOCHLADEN

Zuerst von der Korrektheit des Schlüssels und der Zuordnung zur betreffenden Person überzeugen!

- Seahorse → GnuPG-Schlüssel → Rechtsklick auf betreffenden Schlüssel → Eigenschaften → Reiter „Vertrauen“ → Diesen Schlüssel signieren → Vertrauensstufe und Optionen wählen → Signieren
- Seahorse → GnuPG-Schlüssel → betreffende(n) Schlüssel markieren → Entfernt → Schlüssel abgleichen und veröffentlichen → Abgleichen

BESITZERVERTRAUEN FESTLEGEN

- Seahorse → GnuPG-Schlüssel → Rechtklick auf betreffenden Schlüssel → Eigenschaften → Reiter „Deatails“ → Angaben zum Vertrauen → Stufe wählen

Dabei gilt:

- frisch importierte Schlüssel haben immer Stufe Unbekannt
- Stufe Absolut kann nur für eigene Schlüssel vergeben werden
- Stufe Vollkommen für Personen, zu denen man auch im realen Leben volles Vertrauen hat, deren Schlüssel man überprüft hat und die dafür bekannt sind, sorgsam mit Schlüsseln umzugehen, insbesondere auch beim Signieren fremder Schlüssel.
- Stufe Geringfügig für Personen, die man kennt und deren Schlüssel man überprüft hat
- Stufe Unbekannt behalten, wenn man keine Aussage treffen kann
- Stufe Nie für alle anderen

SCHLÜSSEL VON KOMMUNIKATIONSPARTNERN LÖSCHEN

- Seahorse → GnuPG-Schlüssel → Rechtsklick auf betreffende(n) Schlüssel → Löschen → Löschen

EINRICHTUNG

- Evolution 3.8 wird derzeit (12.11.2013) nur in Englisch ausgeliefert. Falls installiert kann man als Workaround die Sprachdateien von Version 3.6 umbenennen:

```
sudo mv
/usr/share/locale-langpack/de/LC_MESSAGES/evolution-3.6.mo
/usr/share/locale-langpack/de/LC_MESSAGES/evolution-3.8.mo
sudo mv
/usr/share/locale-langpack/de/LC_MESSAGES/evolution-data-server-3.6.mo
/usr/share/locale-langpack/de/LC_MESSAGES/evolution-data-server-3.8.mo
```

- Konten in Evolution einrichten: Evolution → Assistent startet beim ersten Start von Evolution automatisch und ist selbsterklärend, sonst unter Evolution → Bearbeiten → Einstellungen → E-Mail-Konten → Hinzufügen ein neues Konto einrichten (gleicher Assistent wie beim ersten Start)

EINRICHTUNG

- ID des eigenen Schlüssels ermitteln: Seahorse → GnuPG → Rechtsklick auf eigenen Schlüssel → Eigenschaften → Eigentümer → Schlüsselkennung
- Verschlüsselung in betreffendem Konto aktivieren: Evolution → Bearbeiten → Einstellungen → E-Mail-Konten → betreffendes Konto → Bearbeiten → Sicherheit → OpenPGP Schlüssel-Kennung → ID des eigenen Schlüssels eintragen
- Empfehlung: zusätzliches Verschlüsseln mit eigenem Schlüssel aktivieren, sonst landen unlesbare Nachrichten im Postausgang: Evolution → Bearbeiten → Einstellungen → E-Mail-Konten → betreffendes Konto → Bearbeiten → Sicherheit → Haken bei „Beim Verschicken verschlüsselter E-Mails immer für mich selbst verschlüsseln“ setzen

VERSCHLÜSSELTE UND/ODER SIGNIERTE E-MAILS VERSENDEN

- Auf verschlüsselte/unterschriebene E-Mails wird standardmäßig verschlüsselt/unterschrieben geantwortet.
- Evolution → Neu → Optionen → mit PGP signieren / mit PGP verschlüsseln

WEITERE INFORMATIONEN

[1] URL: https://emailselfdefense.fsf.org/de/.

[2] URL: http://www.gnupg.org.

[3] URL: https://wiki.kairaven.de/open/krypto/gpg/gpganleitung.

[4] URL: http://www.hauke-laging.de/sicherheit/openpgp.html.

[5] URL: http://www.selbstdatenschutz.info.

[6] URL: http://www.thunderbird-mail.de/wiki/Enigmail.

[7] URL: http://wiki.ubuntuusers.de/GnuPG.

VIELEN DANK! – NOCH FRAGEN?

- sandigf@mailserver.tu-freiberg.de
- Ekkehardt in #flux auf secundus.stunet.tu-freiberg.de
- Präsentation unter `http://sandig-fg.de`