Carsten Knoll[1], Joschka Heinrich (HG KRETA, Folien)

Sichere Kommunikation: Warum & Wie

22. Januar 2018

[1] casten.knoll@posteo.de

FSFW – Freie Software und Freies Wissen

- Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, . . .)
- Warum machen wir das? Aus Überzeugung!
  - *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)

FSFW – Freie Software und Freies Wissen

- Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, . . .)
- Warum machen wir das? Aus Überzeugung!
  - *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
  - *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrende Summen von Zeitschriften-Verlagen gekauft werden müssen

FSFW – Freie Software und Freies Wissen

- Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, . . .)
- Warum machen wir das? Aus Überzeugung!
  - *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
  - *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrende Summen von Zeitschriften-Verlagen gekauft werden müssen
- Bisherige Projekte
  - Linux-Install-Party, Linux-Presentation-Day
  - Monatliche Sprechstunde zu LaTeX u.a.
  - Programmpapier
  - „Uni-Stick“: 100 × 8 GB mit freier Software
  - Verschlüsselungsgewinnspiel

FSFW – Freie Software und Freies Wissen

- Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, . . .)
- Warum machen wir das? Aus Überzeugung!
  - *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
  - *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrende Summen von Zeitschriften-Verlagen gekauft werden müssen
- Bisherige Projekte
  - Linux-Install-Party, Linux-Presentation-Day
  - Monatliche Sprechstunde zu LaTeX u.a.
  - Programmpapier
  - **„Uni-Stick“: 100 × 8 GB mit freier Software**
  - Verschlüsselungsgewinnspiel

FSFW – Freie Software und Freies Wissen

- Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, . . .)
- Warum machen wir das? Aus Überzeugung!
  - *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
  - *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrende Summen von Zeitschriften-Verlagen gekauft werden müssen
- Bisherige Projekte
  - Linux-Install-Party, Linux-Presentation-Day
  - Monatliche Sprechstunde zu LaTeX u.a.
  - Programmpapier
  - **„Uni-Stick“: 100 × 8 GB mit freier Software**
  - Verschlüsselungsgewinnspiel

FSFW – Freie Software und Freies Wissen

- Hochschulgruppe seit 2014, ca. 10 Leute (TU, HTW, . . .)
- Warum machen wir das? Aus Überzeugung!
  - *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
  - *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrende Summen von Zeitschriften-Verlagen gekauft werden müssen
- Bisherige Projekte
  - Linux-Install-Party, Linux-Presentation-Day
  - Monatliche Sprechstunde zu LaTeX u.a.
  - Programmpapier
  - „Uni-Stick“: 100 × 8 GB mit freier Software
  - Verschlüsselungsgewinnspiel

- Für (Mitmachen-)Interessierte: `https://fsfw-dresden.de`

Ablauf

1) Verschlüsselung in der Theorie

- Narrativ-Dekonstruktion: „Ich habe doch nichts zu verbergen“
- Schutzziele sicherer Kommunikation
- Funktionsweise PGP

Ablauf

1) Verschlüsselung in der Theorie

- Narrativ-Dekonstruktion: „Ich habe doch nichts zu verbergen“
- Schutzziele sicherer Kommunikation
- Funktionsweise PGP

2) PGP in der Praxis

- Installation (individuell)
- Schlüsselgenerierung
- E-Mails verschlüsseln
- Ausblick

Narrativ: „Ich habe doch nichts zu verbergen“

- Weit verbreitet und sehr wirkmächtig
- Sollte oft und fundiert widersprochen werden

Narrativ: „Ich habe doch nichts zu verbergen“

- Weit verbreitet und sehr wirkmächtig
- Sollte oft und fundiert widersprochen werden
- Stichworte
  - Kriminalität (Einbruch, Erpressung, . . .)
  - Privatsphäre
  - Selbstzensur (analog: Kamera-Attrappen)
  - Schutzwürdige Daten (Gesundheit, Geschäftsgeheimnisse)
  - Demokratie
  - Journalismus
  - Whistleblowing
  - Erstarken totalitärer Strukturen

„Ich habe doch nichts zu verbergen“

- In Menschheitsgeschichte:
  viele Beispiele für **rücksichtslosen Egoismus**
- „Wissen ist Macht“

$\Rightarrow$ sensibler Umgang mit Informationen empfehlenswert

„Ich habe doch nichts zu verbergen“

- In Menschheitsgeschichte:
  viele Beispiele für **rücksichtslosen Egoismus**
- „Wissen ist Macht“

$\Rightarrow$ sensibler Umgang mit Informationen empfehlenswert

- **Digitalisierung verstärkt das Problem**
- E-Mail[1] ist wie Postkarte: unterwegs[2] lesbar
- E-Mail ist noch schlimmer als Postkarte:
  - automatisiert auswertbar
  - unbemerkt kopierbar
  - unbemerkt veränderbar (inkl. Metadaten, bspw. Absender)

1: E-Mail = nur Beispielmedium 2: ggf. um die ganze Welt

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
  $\rightarrow$ A weiß, nur B kann Nachricht lesen

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
  $\rightarrow$ A weiß, nur B kann Nachricht lesen
- **Integrität**
  $\rightarrow$ B weiß, die Nachricht ist nur von A geschrieben und nicht verändert wurden

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
  → A weiß, nur B kann Nachricht lesen
- **Integrität**
  → B weiß, die Nachricht ist nur von A geschrieben und nicht verändert wurden
- **Anonymität**
  → A bestimmt, wem eigene Identität preisgegeben wird

Schutzziele sicherer Kommunikation

- **Vertraulichkeit**
  → A weiß, nur B kann Nachricht lesen
- **Integrität**
  → B weiß, die Nachricht ist nur von A geschrieben und nicht verändert wurden
- **Anonymität**
  → A bestimmt, wem eigene Identität preisgegeben wird
- **Verfügbarkeit**
  → obige Schutzziele werden in annehmbarer Zeit realisiert

PGP – Begriffe

- asymmetrische Verschlüsselung
- Privater Schlüssel (*private key*)
- Öffentlicher Schlüssel (*public key*)
- GPG vs. PGP

PGP – Begriffe

- asymmetrische Verschlüsselung
- Privater Schlüssel (*private key*)
- Öffentlicher Schlüssel (*public key*)
- GPG vs. PGP
- Schlüsselserver (*keyserver*)
- Fingerabdruck
- Metadaten
- Widerrufszertifikat

PGP – Das Problem

- *P1:* A möchte Nachricht an B vertraulich schicken

$\Rightarrow$ Nachricht verschlüsseln

PGP – Das Problem

- *P1:* A möchte Nachricht an B vertraulich schicken

$\Rightarrow$ Nachricht verschlüsseln

- *P2:* Schlüsselverteilung

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren (PGP)

  - Es gibt: **Ö**ffentlichen **S**chlüssel und **P**rivaten **S**chlüssel

PGP – Das Problem

- *P1:* A möchte Nachricht an B vertraulich schicken

$\Rightarrow$ Nachricht verschlüsseln

- *P2:* Schlüsselverteilung

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren (PGP)

  - Es gibt: **Ö**ffentlichen **S**chlüssel und **P**rivaten **S**chlüssel
  - **ÖS**: zum Verschlüsseln

  - **PS**: zum Entschlüsseln

PGP – Das Problem

- *P1:* A möchte Nachricht an B vertraulich schicken

$\Rightarrow$ Nachricht verschlüsseln

- *P2:* Schlüsselverteilung

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren (PGP)

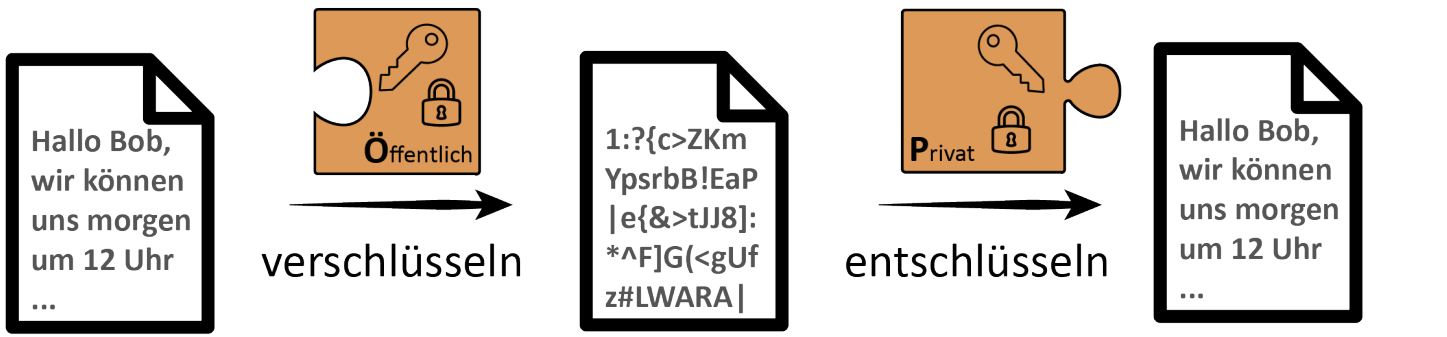
  - Es gibt: **Ö**ffentlichen **S**chlüssel und **P**rivaten **S**chlüssel
  - **ÖS**: zum Verschlüsseln

  - **PS**: zum Entschlüsseln

Oft eingesetzte, freie Implementierung: GPG (**G**NU **P**rivacy **G**uard, 1999)

Nicht freier Vorläufer & Namensgeber des Verfahrens: PGP (**P**retty **G**ood **P**rivacy, 1991)

PGP – Funktionsweise 1



Daten
(Nachricht im Klartext)

verschlüsselte Daten

ursprüngliche Daten

PGP – Funktionsweise 2

- Öffentlicher Schlüssel („public key“)
  - Benötigt zum Verschlüsseln
  - Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
  - kann/sollte man weitergeben → auf Keyserver hochladen

    Bsp: `http://pgp.mit.edu` zu bedenken: nicht löschbar, nur widerrufbar ⇒ Anonymität gefährdet

PGP – Funktionsweise 2

- Öffentlicher Schlüssel („public key“)
  - Benötigt zum Verschlüsseln
  - Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
  - kann/sollte man weitergeben → auf Keyserver hochladen

    Bsp: `http://pgp.mit.edu` zu bedenken: nicht löschbar, nur widerrufbar ⇒ Anonymität gefährdet
- Privater Schlüssel („private key“)
  - Benötigt zum Entschlüsseln
  - Darf nicht verloren gehen
    → Entschlüsseln wäre dann unmöglich
  - Darf nicht in fremde Hände kommen
    → andere können meine Mails entschlüsseln
  - Typischerweise nochmal zusätzlich mit einem Passwort verschlüsselt

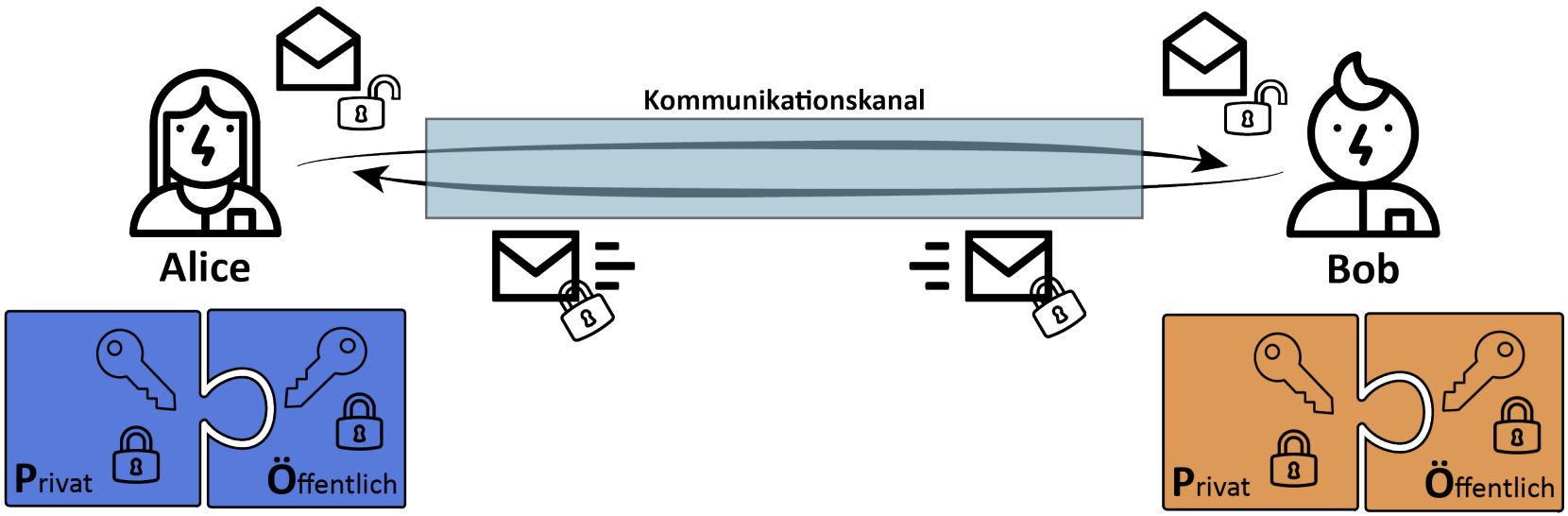
PGP – Funktionsweise 2

- Öffentlicher Schlüssel („public key“)
  - Benötigt zum Verschlüsseln
  - Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
  - kann/sollte man weitergeben → auf Keyserver hochladen

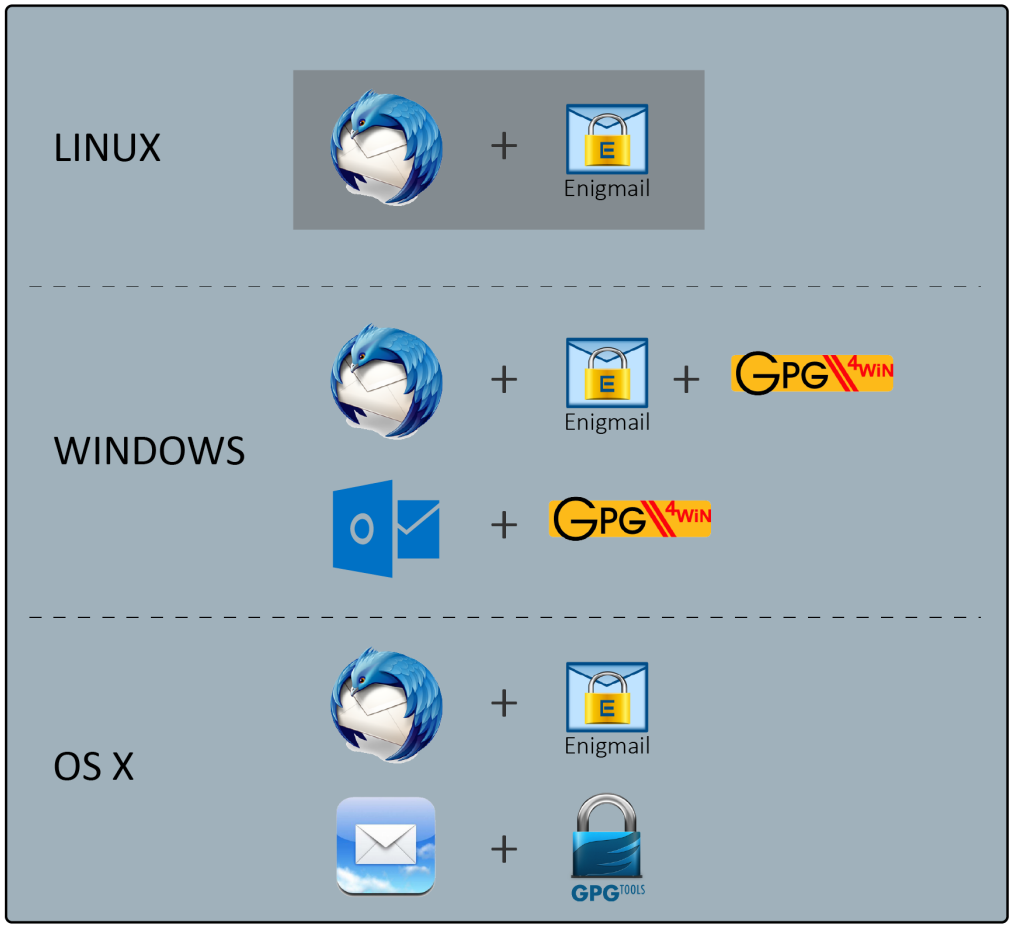
    Bsp: `http://pgp.mit.edu` zu bedenken: nicht löschbar, nur widerrufbar ⇒ Anonymität gefährdet
- Privater Schlüssel („private key“)
  - Benötigt zum Entschlüsseln
  - Darf nicht verloren gehen
    → Entschlüsseln wäre dann unmöglich
  - Darf nicht in fremde Hände kommen
    → andere können meine Mails entschlüsseln
  - Typischerweise nochmal zusätzlich mit einem Passwort verschlüsselt

⇒ Sicheres Backup wichtig

PGP – Funktionsweise 3



Praxisteil – Installation 1



- Anleitungen: `https://fsfw-dresden.de/gpg`

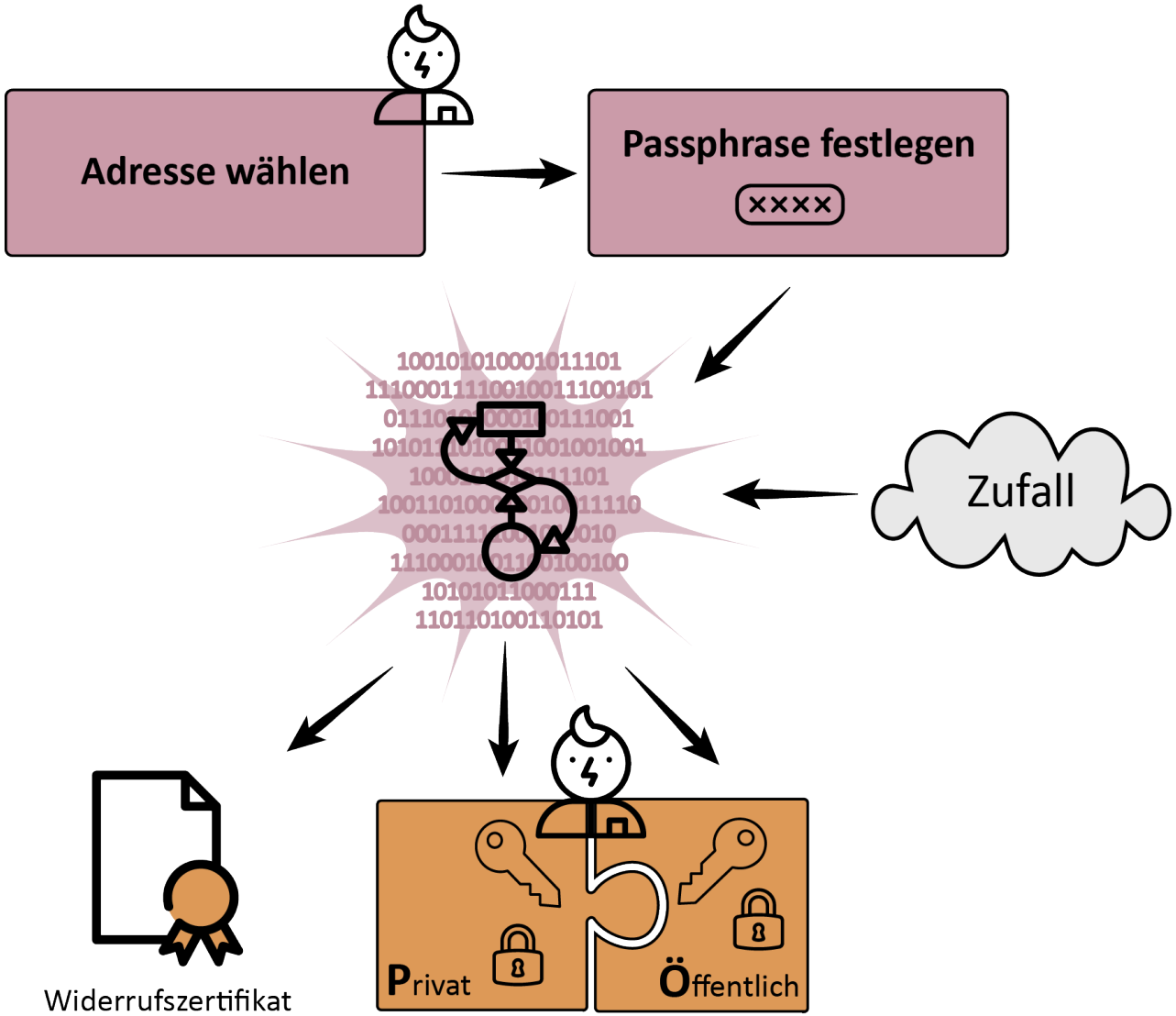
Praxisteil – Installation 2

- Anleitungen: `https://fsfw-dresden.de/gpg`

- Bei Bedarf temporäre E-Mailadressen zum Test:
  - Adresse: `tmp01@alnilam.uberspace.de` ... `tmp05@...`
  - Username: `plq-tmp01` ... `plq-tmp05`
  - Mailserver: `alnilam.uberspace.de`
  - IMAP, Port: 993
  - Passwort: `signatur`

  - werden heute Abend wieder gelöscht

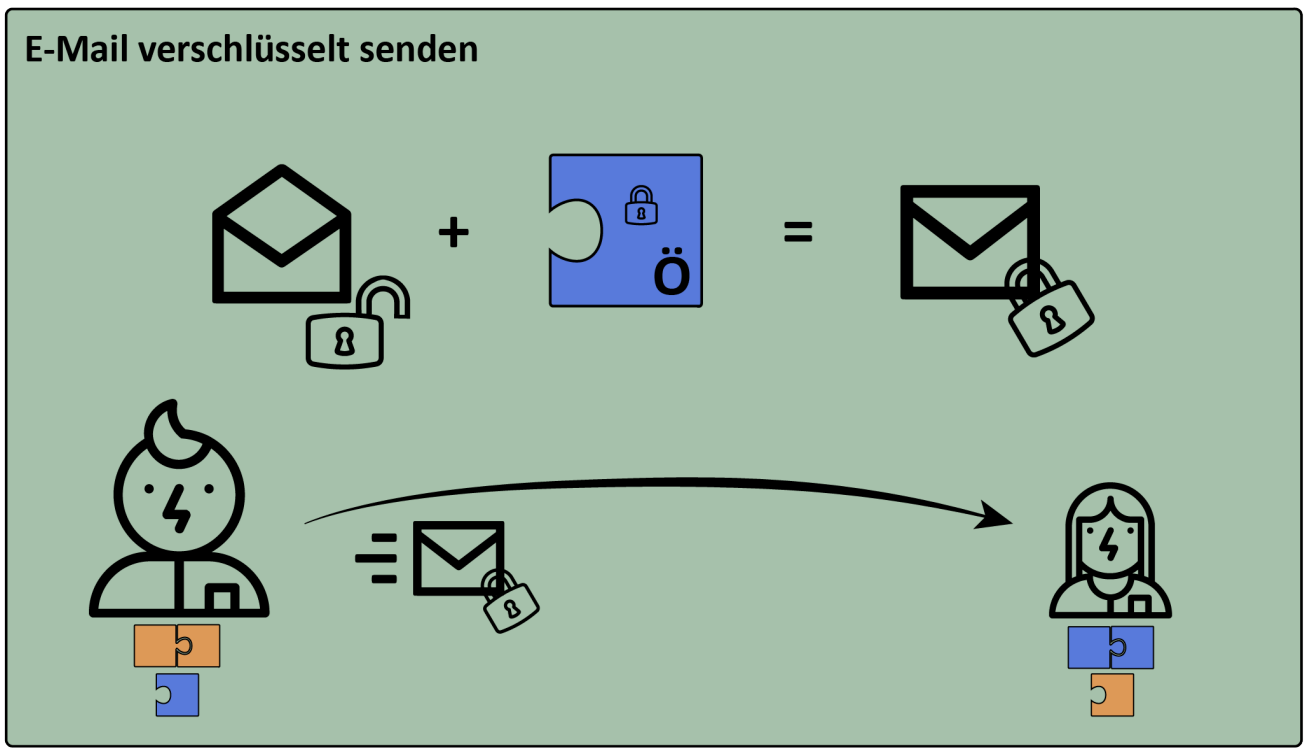
Schlüsselgenerierung



E-Mails verschlüsseln

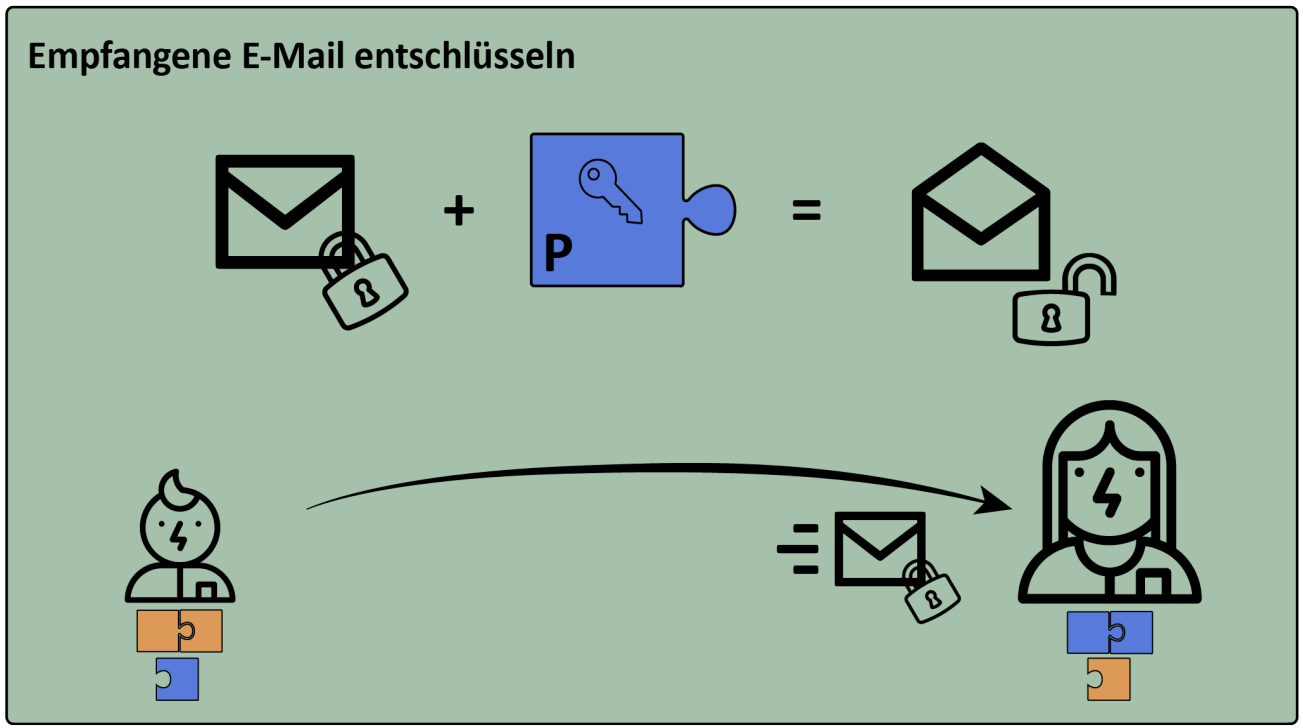
- ÖS der Empfängerin muss bereits bekannt sein, z.B. via
  - Schlüsselserver
  - Direkte Veröffentlichung

Enigmail → Key Management → Edit → Import from Clipboard



Testmail (mit Schlüssel im Anhang) an: `carsten.knoll@posteo.de`

E-Mails entschlüsseln



Ausblick – Schutzziele bei PGP

- ☐ Vertraulichkeit
- ☐ Integrität (keine Veränderung)
- ☐ Anonymität
- ☐ Verfügbarkeit

Ausblick – Schutzziele bei PGP

- ☑ Vertraulichkeit → Verschlüsselung
- ☐ Integrität (keine Veränderung)
- ☐ Anonymität
- ☐ Verfügbarkeit

Ausblick – Schutzziele bei PGP

- ☑ Vertraulichkeit → Verschlüsselung
- ☐ Integrität (keine Veränderung) → **Signatur notwendig**
- ☐ Anonymität
- ☐ Verfügbarkeit

Ausblick – Signieren 1

- Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- Überprüfen = Entschlüsseln mit ÖS

$\Rightarrow$ Man muss dem öffentlichen Schlüssel vertrauen

☑ Integrität (keine Veränderung)

Ausblick – Signieren 1

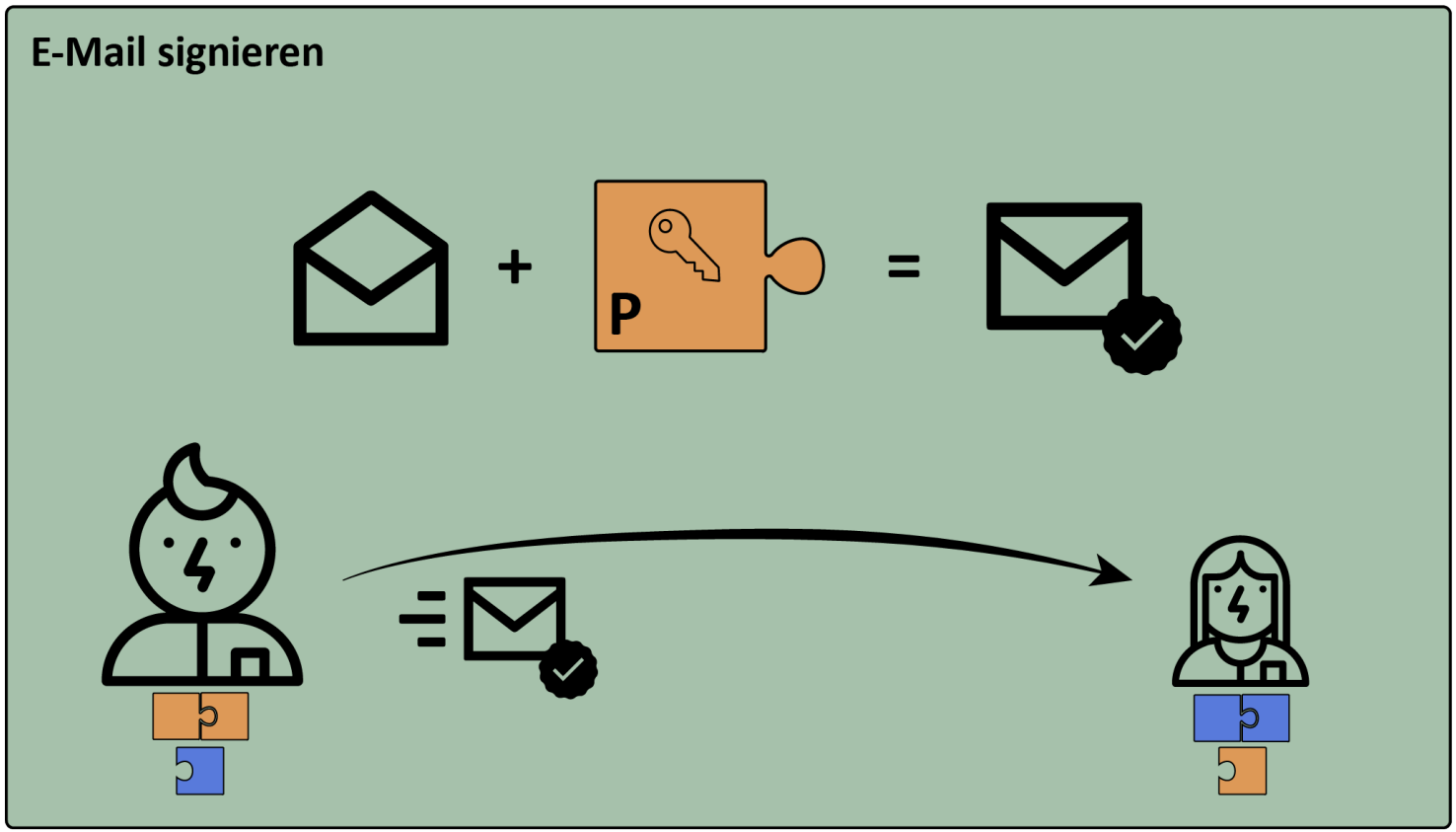
- Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- Überprüfen = Entschlüsseln mit ÖS

$\Rightarrow$ Man muss dem öffentlichen Schlüssel vertrauen

☑ Integrität (keine Veränderung)

- Schlüssel signieren bei persönlichem Treffen (Keysharing-Party) $\rightarrow$ „Web of trust“
- Fingerabdruck-Bsp:
  `214E 4E9D B193 6AF2 CFDC 68DF 13AD 3604` **`9D3E F6BF`**

Ausblick – Signieren 2



Ausblick – Schlüssel pflegen

- Ablaufdatum? $\Rightarrow$ Verlängerung notwendig!
  - $\rightarrow$ ggf. neu auf Schlüsselserver hochladen!

Ausblick – Schlüssel pflegen

- Ablaufdatum? $\Rightarrow$ Verlängerung notwendig!
  - $\rightarrow$ ggf. neu auf Schlüsselserver hochladen!

- Widerrufszertifikat sichern
  - $\rightarrow$ wir benötigt falls:
    - Passphrase vergessen
    - PS verloren ($\rightarrow$ Backup!)
    - Vertrauen in PS verloren

Ausblick – Nachteile PGP

Was wird verschlüsselt?

- Text
- Anhänge Format-Empfehlung: `PGP/MIME` nicht: `Inline PGP`

Was wird nicht verschlüsselt?

- Metadaten
  - Absender*in, Empfänger*in, **Betreff**, ...

Weiterführendes

PGP-Verschlüsselung für Webmail

- `https://vimeo.com/178702500` (Screencast)
- Anleitung von Posteo

Allgemeine Infos

- `https://virtual-privacy.org`

Cryptopartys

- `https://www.cryptoparty.in`
- `https://de.wikipedia.org/wiki/CryptoParty`

Radio

- Deutschlandfunk-Essay: *Niemand hat nichts zu verbergen*

Videos

- G. Greenwald: *Why privacy matters*
- J. Oliver + E. Snwoden (lustig)

https://fsfw-dresden.de

Plenum: Do. (ungerade KW, SLUB)