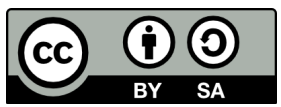
Cryptoparty

Michael Weiner

24.09.2018



Fahrplan

Fahrplan

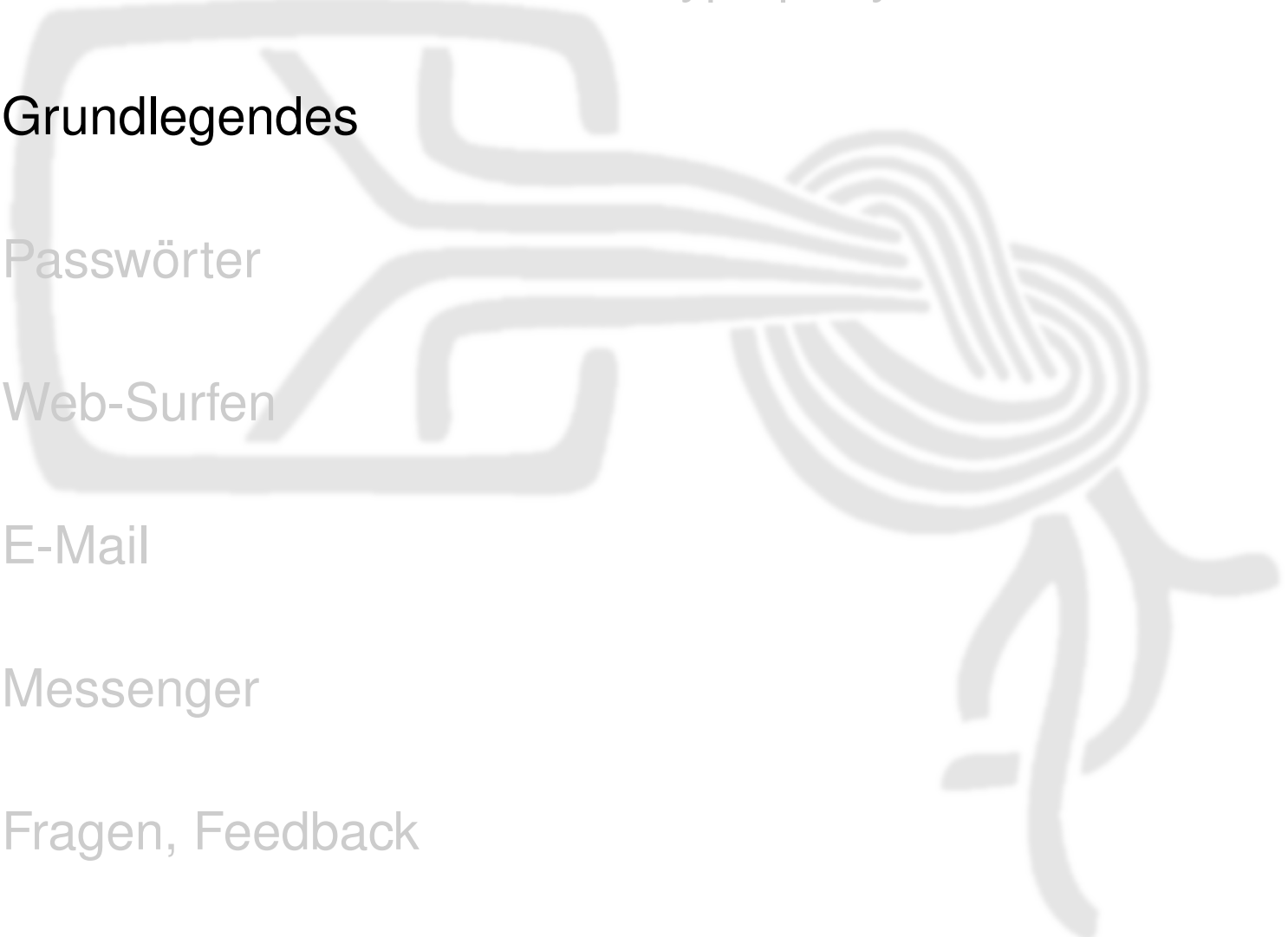
Die Veranstalter

- Chaos Computer Club München e.V.
- Forum InformatikerInnen für Frieden
  und gesellschaftliche Verantwortung e.V.
- Medienzentrum München (MZM)
  Institut für Medienpädagogik in Forschung und Praxis
  JFF – Jugend Film Fernsehen e.V.

Die Cryptoparty

- Weltweite Bewegung von technisch interessierten
- Ziel: Datensicherheit für jedermann
- Themen sind z.B.
  - Kommunikation: E-Mail, Anrufe, Chat
  - Datenspeicherung und -weitergabe
  - Veröffentlichen von Informationen
  - Passwörter
- Aus Zeitgründen beschränken wir uns heute auf
  - Passwort-Management
  - Anonyme(re)s Web-Surfen
  - E-Mail-Verschlüsselung und -Signatur
  - . . . und mehr auf Anfrage, wenn noch Zeit ist

Fahrplan



Warnhinweise

- 100% Sicherheit gibt es nicht
- Absichern heißt, Angriffe *teurer* zu machen
  - Die Kosten für den Angriff müssen den Wert der Daten übersteigen
  - Ein Angriff darf sich nicht mehr *lohnen*
  - Problem: Wert wird oft unterschätzt
- Was wir hier zeigen, ist ein Anfang
  - Hilft dagegen, als „Beifang“ zu enden
  - Gegen gezielte Angriffe – auch durch Verwechslung – benötigt es deutlich mehr
- Irren ist menschlich – auch was die Inhalte der folgenden Folien betrifft :-)

Leitfragen

- *Was* soll sichergestellt werden?
  - Eigene Anonymität
  - Echtheit des Gegenübers (Authentizität)
  - Unverfälschtheit der Nachricht (Integrität)
  - Geheimhaltung der Nachricht (Vertraulichkeit)
  - …
- *Wem* vertraut Ihr?

Vertrauen

Woher weiß man, wem man vertrauen kann?

- Kurze Antwort: weiß man *nicht*
- Lange Antwort
  - es gibt Fragen, die man stellen kann. . .
  - . . . und es gibt das Bauchgefühl

Welche Fragen kann man stellen?

Beispiel: *Wo* sind meine Daten?

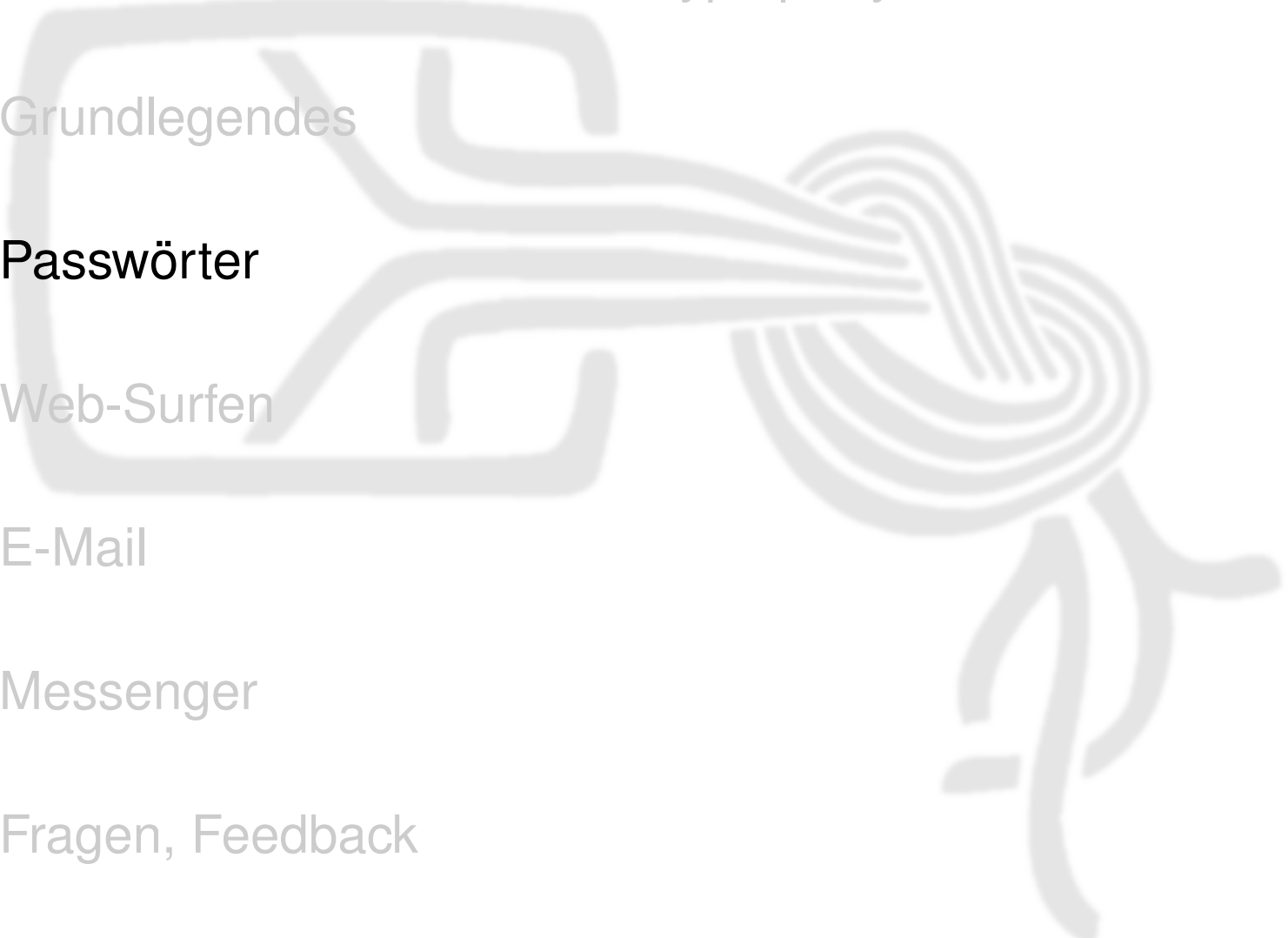
- Auf einem Blatt Papier zuhause in meiner Schublade.
- Auf meinem Computer:
  - Wie gut ist die Software *überprüfbar*, die meine Daten verwaltet?
    - Open Source (in menschenlesbarer Form öffentlich): gut überprüfbar
    - Closed Source (menschenlesbare Form geheim): quasi nicht überprüfbar
- In der Cloud
  - *Wer* betreibt einen Dienst?
  - Womit *verdient* der Betreiber sein *Geld*?
  - Wem könnten die Daten *nutzen* oder *schaden*?
  - Was *lernt* der Betreiber über mich?

Meta- und Nutzdaten

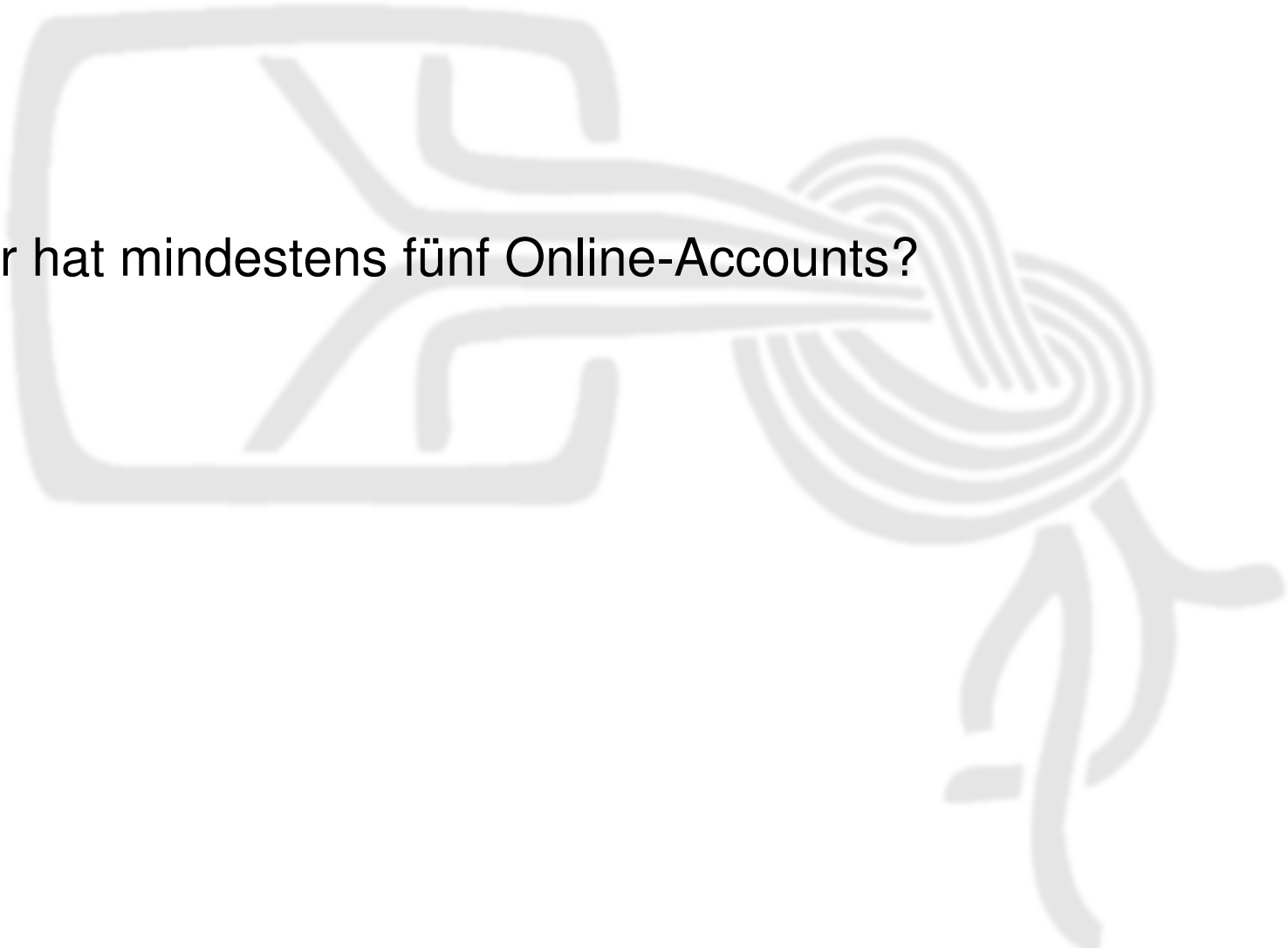
- Meta-/Verbindungsdaten (“Briefumschlag”)
  - Absender, Empfänger, Betreff einer E-Mail
  - Besuch und Aufenthaltsdauer auf einer Webseite
  - Wer, wann, wie lange mit wem telefoniert
  - Aufenthaltsort von Mobiltelefonen: Bewegungsprofil!
- Nutz-/Inhaltsdaten (“Brief”)
  - E-Mail-Text und -Anhänge
  - Webseiten-Inhalte
  - Gesprochene Sprache beim Telefonieren
  - SMS-Inhalt

Metadaten zu verschlüsseln ist nicht möglich,
sie zu verschleiern schwierig.

Fahrplan

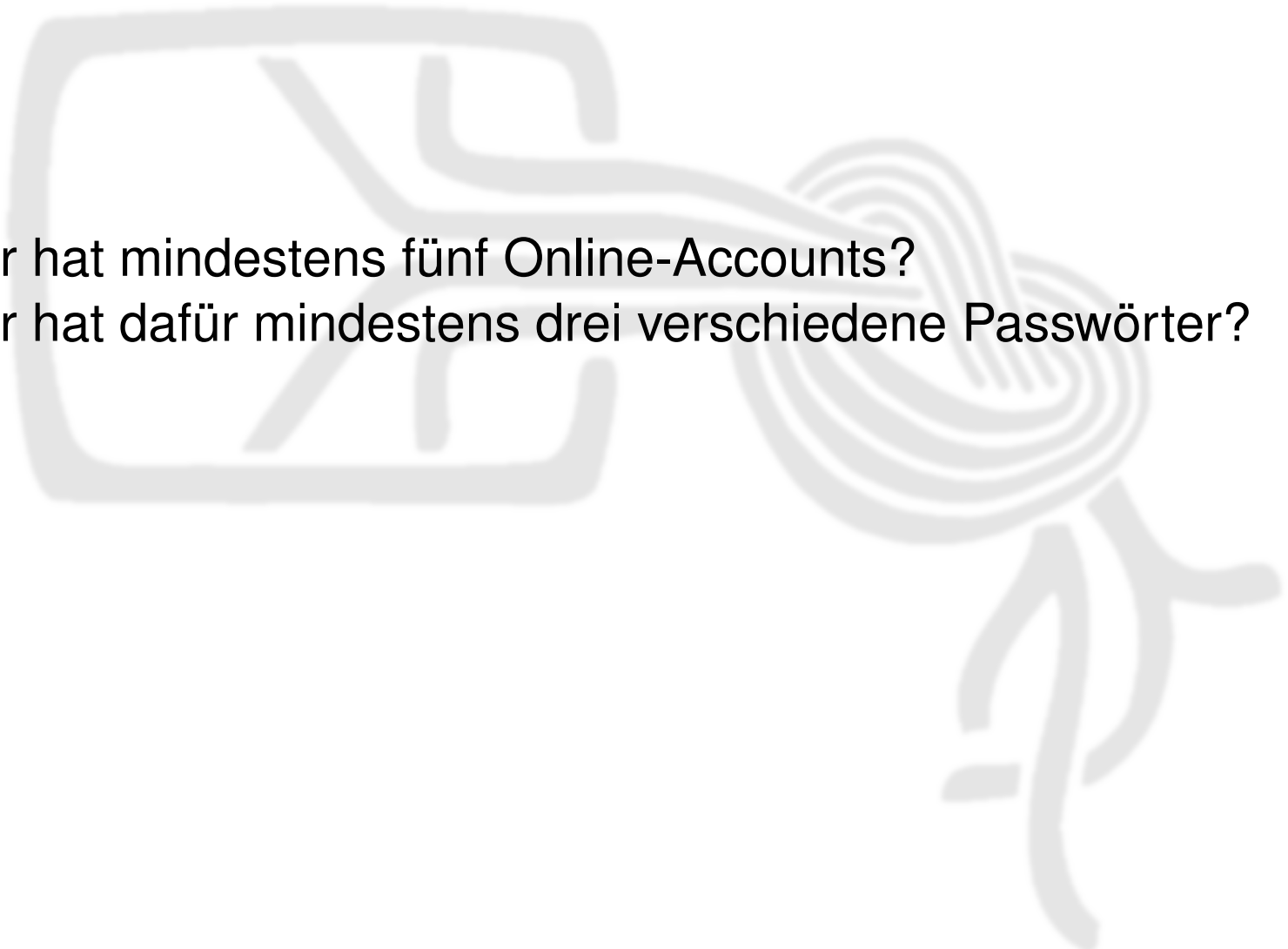


Passwörter



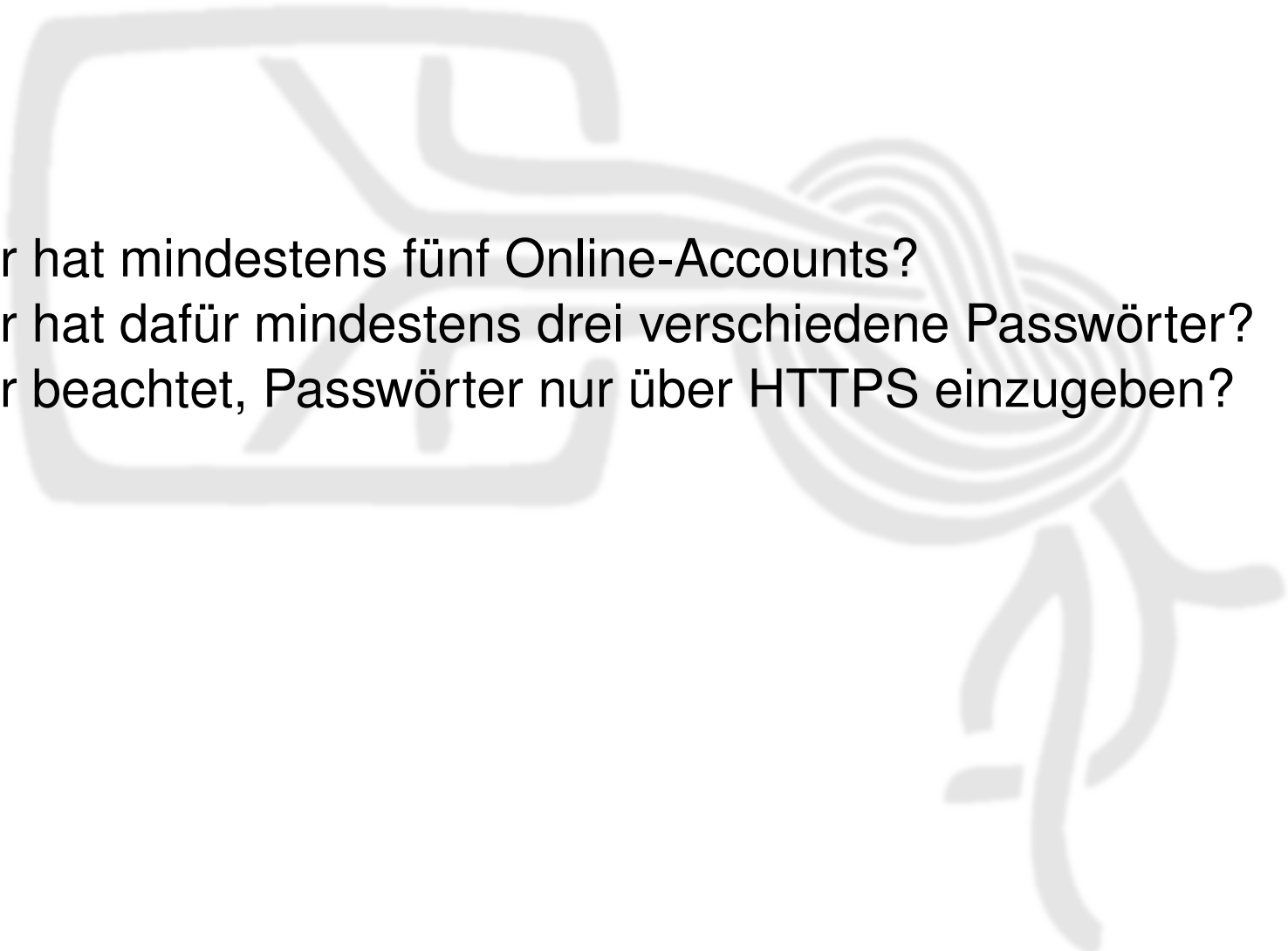
Wer hat mindestens fünf Online-Accounts?

Passwörter



Wer hat mindestens fünf Online-Accounts?
Wer hat dafür mindestens drei verschiedene Passwörter?

Passwörter

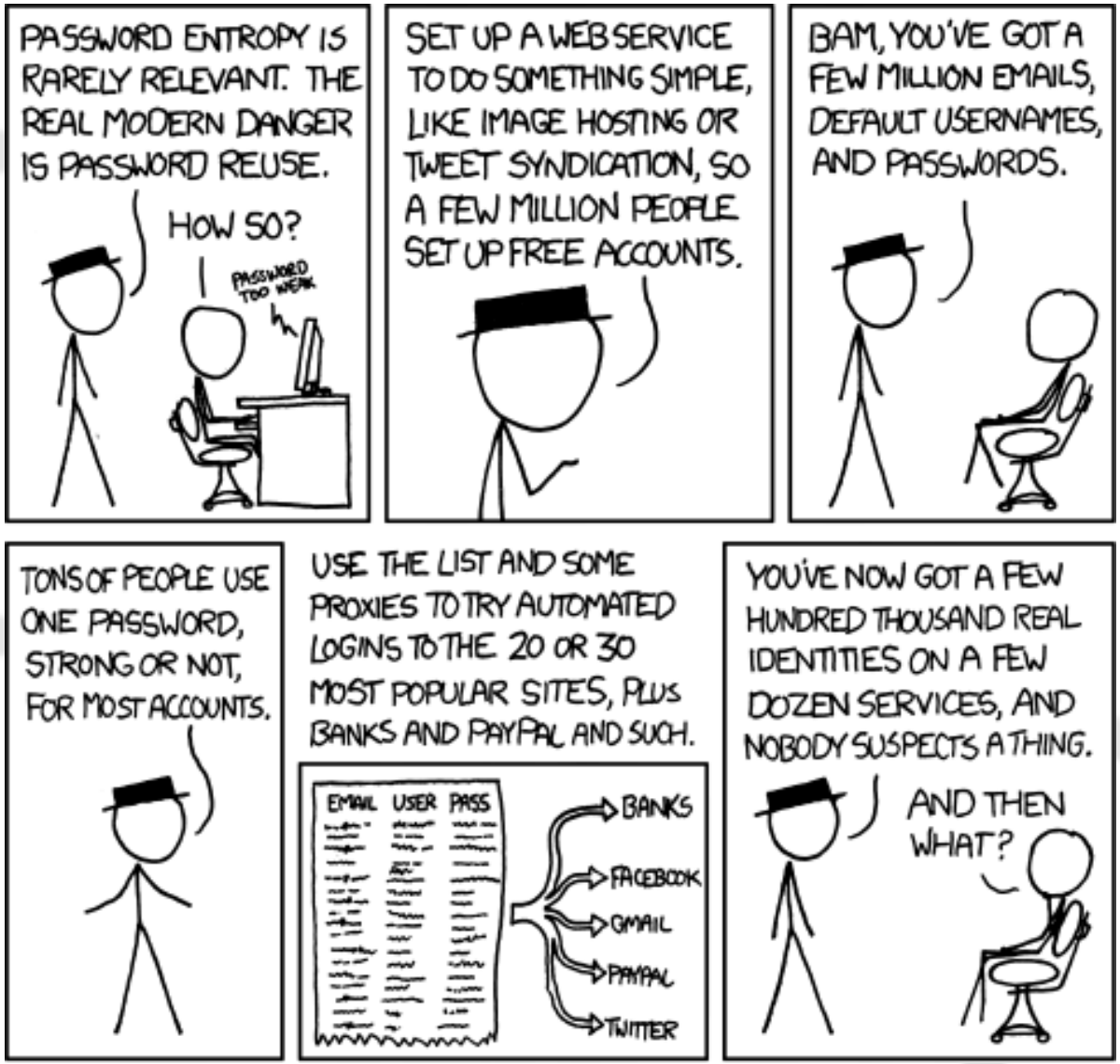


Wer hat mindestens fünf Online-Accounts?
Wer hat dafür mindestens drei verschiedene Passwörter?
Wer beachtet, Passwörter nur über HTTPS einzugeben?

Anzahl Passwörter

- Zugangsdaten werden bei Hackerangriffen auf Diensteanbieter gestohlen
  - Angreifer probieren Zugangsdaten auch anderswo aus
  - Schaden lässt sich begrenzen, wenn Benutzername und Passwort nur bei diesem einen Anbieter passen
- Besonders wichtig: E-Mail-Accounts
  - Weil „Passwort zurücksetzen“ oft via E-Mail
  - Wer den E-Mail Account übernommen hat, kann dadurch sämtliche Accounts übernehmen
- Ideal: Für jeden Anbieter anderes Passwort
- Alternative: Passwörter „salzen“
  - *passwort*.amz für Onlineshop a
  - *passwort*.zal für Onlineshop z
  - *anderespasswort* für Mails

Passwort Wiederverwertung



Bildquelle: Ausschnitt aus xkcd: Password Reuse / CC BY-NC 2.5

Sichere Passwörter

Anforderungen

- Klein- und Großbuchstaben, Zahlen,
  begrenzt: Sonderzeichen
- Wichtiger: Lang genug!

Merkbarkeit

- Pass*satz* statt Passwort
  Beispiel: `margaretthatcheris110%SEXY`
  (aus Snowden-Interview: `https://www.youtube.com/watch?v=yzGzB-yYKcc`)
- würfeln, dann sieben zufällige Wörter verwenden
  siehe `https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/`

Passwort-Manager

Passwort-Manager verwalten Passwörter in einer verschlüsselten Datenbank; der Anwender muss sich idealerweise nur das Datenbank-Passwort merken.

Passwort-Manager

Passwort-Manager verwalten Passwörter in einer verschlüsselten Datenbank; der Anwender muss sich idealerweise nur das Datenbank-Passwort merken.

Vorteile

- erzeugt statistisch zufällige Passwörter
- ermöglicht es, jedes Passwort nur einmal zu verwenden

Passwort-Manager

Passwort-Manager

Passwort-Manager verwalten Passwörter in einer verschlüsselten Datenbank; der Anwender muss sich idealerweise nur das Datenbank-Passwort merken.

Vorteile

- erzeugt statistisch zufällige Passwörter
- ermöglicht es, jedes Passwort nur einmal zu verwenden

Nachteil

- Eingefangene Malware bekommt alle Passwörter auf einmal
  allerdings: auch ohne Passwort-Manager kann Malware Tastatureingaben mitlesen

Passwort-Manager

Passwort-Manager

Passwort-Manager verwalten Passwörter in einer verschlüsselten Datenbank; der Anwender muss sich idealerweise nur das Datenbank-Passwort merken.

Vorteile

- erzeugt statistisch zufällige Passwörter
- ermöglicht es, jedes Passwort nur einmal zu verwenden

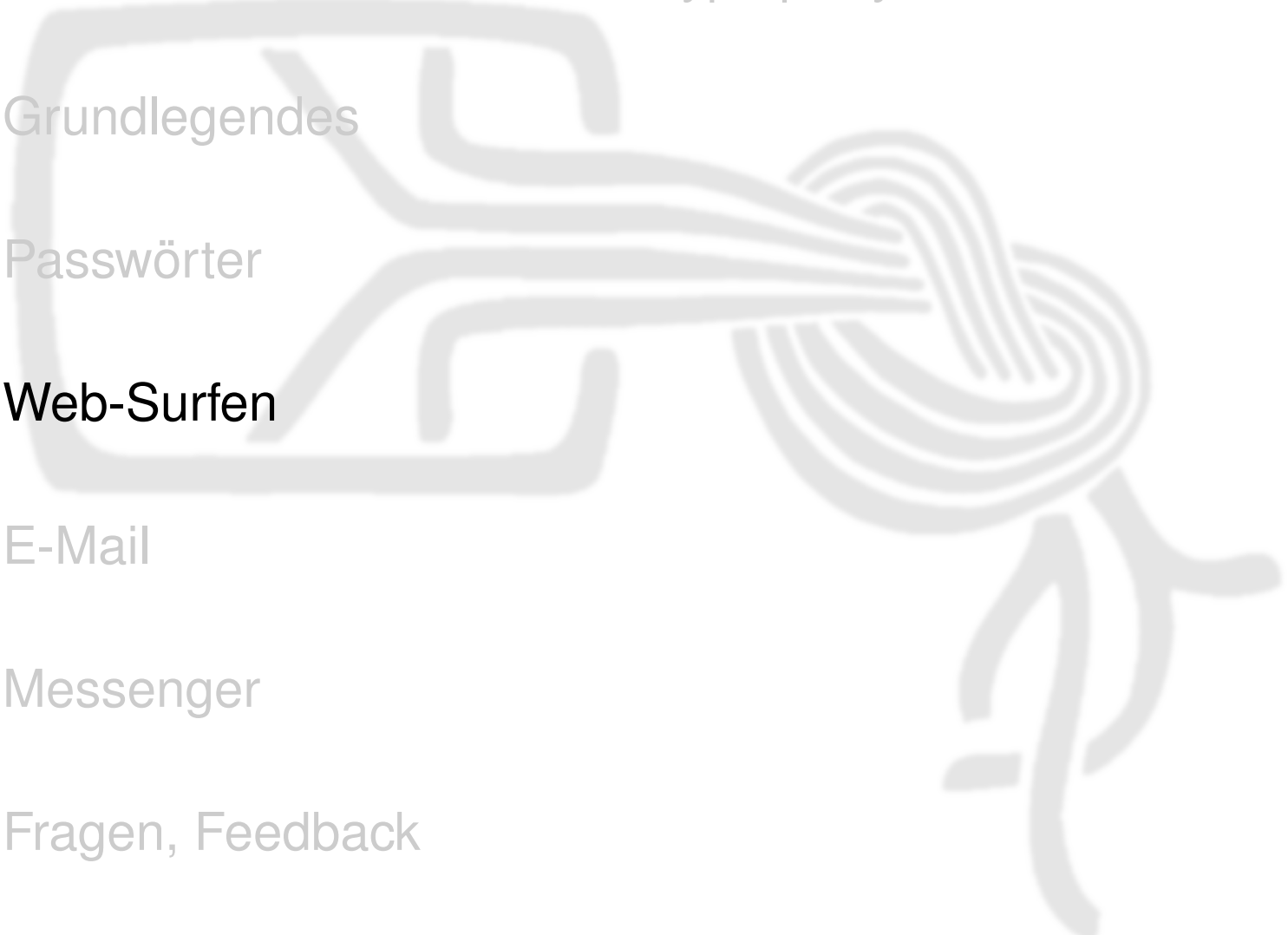
Nachteil

- Eingefangene Malware bekommt alle Passwörter auf einmal
  allerdings: auch ohne Passwort-Manager kann Malware Tastatureingaben mitlesen

Anmerkungen

- Entscheidung zwischen lokalen und “Cloud”-Datenbanken = “klassischer” Tradeoff zwischen Sicherheit und Komfort
- Backups machen – und wichtige Passwörter trotzdem merken!
- unsere Empfehlung: KeePass(X)

Fahrplan



«««< HEAD

Tracking

Ausgangslage

Ein Großteil aller Websites nutzen Drittanbieter für

- Werbung
- “Social Media”-Präsenz
- statistische Analysen
- . . .

Tracking

Ausgangslage

Ein Großteil aller Websites nutzen Drittanbieter für

- Werbung
- “Social Media”-Präsenz
- statistische Analysen
- . . .

Diese Drittanbieter

- bekommen jeden Besuch einer solchen Webseite mit

Tracking

Ausgangslage

Ein Großteil aller Websites nutzen Drittanbieter für

- Werbung
- “Social Media”-Präsenz
- statistische Analysen
- . . .

Diese Drittanbieter

- bekommen jeden Besuch einer solchen Webseite mit
- können Besucher seitenübergreifend identifizieren

Tracking

Ausgangslage

Ein Großteil aller Websites nutzen Drittanbieter für

- Werbung
- “Social Media”-Präsenz
- statistische Analysen
- . . .

Diese Drittanbieter

- bekommen jeden Besuch einer solchen Webseite mit
- können Besucher seitenübergreifend identifizieren
- sind oft Dienstleister für sehr viele Webseiten gleichzeitig

Tracking

Ausgangslage

Ein Großteil aller Websites nutzen Drittanbieter für

- Werbung
- “Social Media”-Präsenz
- statistische Analysen
- . . .

Diese Drittanbieter

- bekommen jeden Besuch einer solchen Webseite mit
- können Besucher seitenübergreifend identifizieren
- sind oft Dienstleister für sehr viele Webseiten gleichzeitig

Ja und?

Tracking

Ausgangslage

Ein Großteil aller Websites nutzen Drittanbieter für

- Werbung
- “Social Media”-Präsenz
- statistische Analysen
- . . .

Diese Drittanbieter

- bekommen jeden Besuch einer solchen Webseite mit
- können Besucher seitenübergreifend identifizieren
- sind oft Dienstleister für sehr viele Webseiten gleichzeitig

Ja und?

- wenige Anbieter lernen sehr viel über jeden Nutzer

Tracking

Ausgangslage

Ein Großteil aller Websites nutzen Drittanbieter für

- Werbung
- “Social Media”-Präsenz
- statistische Analysen
- . . .

Diese Drittanbieter

- bekommen jeden Besuch einer solchen Webseite mit
- können Besucher seitenübergreifend identifizieren
- sind oft Dienstleister für sehr viele Webseiten gleichzeitig

Ja und?

- wenige Anbieter lernen sehr viel über jeden Nutzer
- . . . und verteilen manchmal (unfreiwillig) Schadsoftware

- IP-Adresse
- Cookies und Co (HTML5 Persistent Local Storage, Flashcookies, . . .)
- Browser-Fingerabdruck

  Visualisierung: `https://panopticlick.eff.org/`

Schutzmaßnahmen – Level 1
Nur Einstellungen ändern

- Standardsuchmaschine
  auf datenschutzfreundliche Anbieter ändern, z.B.
  - DuckDuckGo
  - Startpage
- Cookies verbieten oder nur selektiv erlauben
- Plugins auf „Click-to-use“ stellen
- Verlauf beim Beenden löschen

Schutzmaßnahmen – Level 2

Plug-Ins installieren

- Adblocker
- Tracking-Blocker
- Cross-Domain-Request-Blocker
- Referer-Manager
- ...

- Adblocker
- Tracking-Blocker
- Cross-Domain-Request-Blocker
- Referer-Manager
- . . .

Details später in Kleingruppen

Schutzmaßnahmen – Level 3

Neue Programme installieren oder benutzen

- Tor Browser Bundle (Freie Software)
  - Anonymisierung des Webverkehrs durch *„intelligente Umwege“*

    `https://www.torproject.org/about/overview`
  - Fingerabdruck bei allen Tor Browsern identisch
  - Gewählte Plugins vorinstalliert
  - Automatische Updates
  - Hohe Sicherheit, aber prinzipbedingt langsamer
  - **Aufpassen bei**
    - uverschlüsselten Verbindungen – Tor-Knoten (NSA?) können mitlesen
    - Kommunikationspartnern, die einen sowieso kennen

  <++>

Schutzmaßnahmen – Level 3

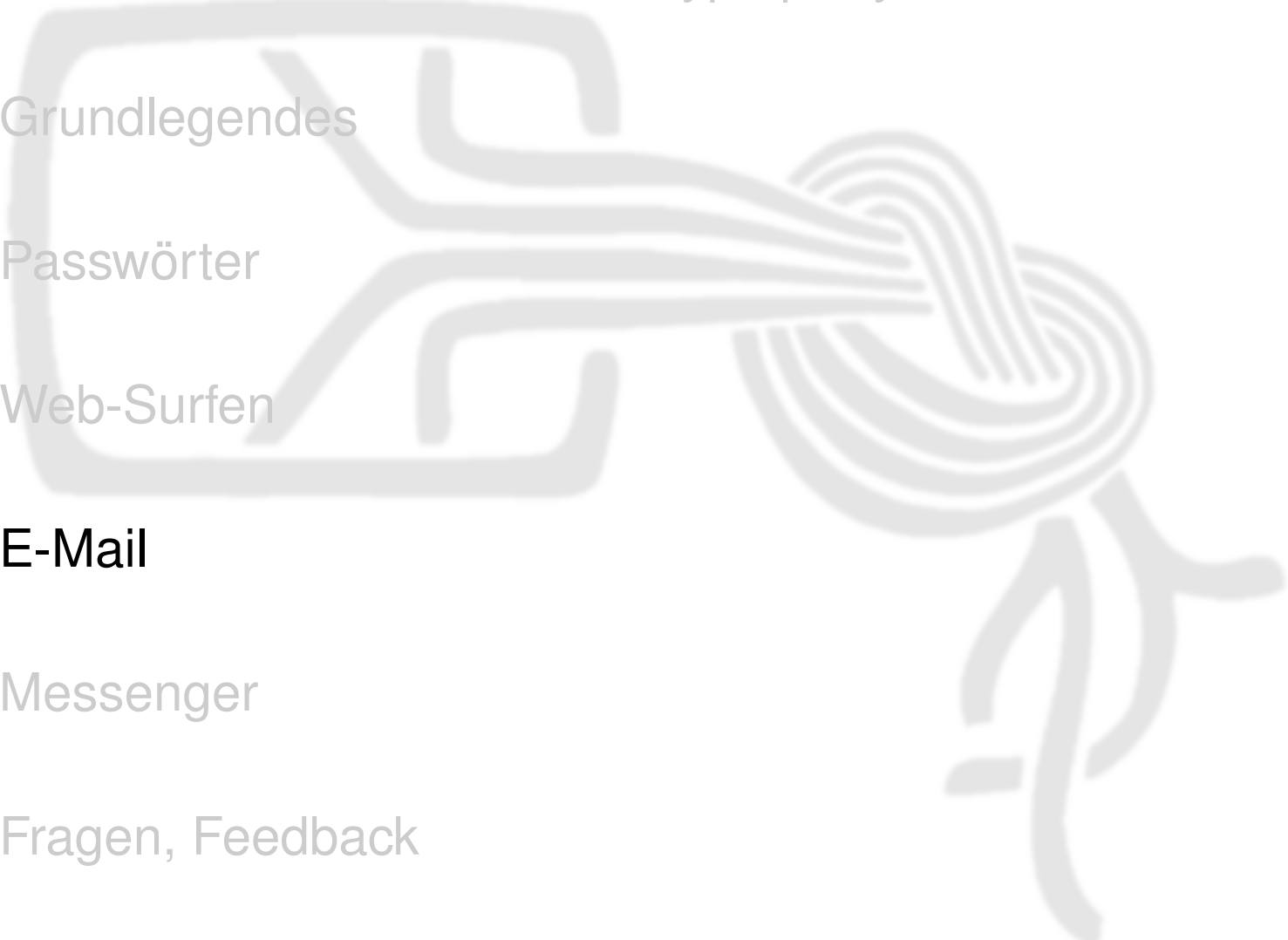
Neue Programme installieren oder benutzen

- Tor Browser Bundle (Freie Software)
  - Anonymisierung des Webverkehrs durch *„intelligente Umwege“*

    `https://www.torproject.org/about/overview`
  - Fingerabdruck bei allen Tor Browsern identisch
  - Gewählte Plugins vorinstalliert
  - Automatische Updates
  - Hohe Sicherheit, aber prinzipbedingt langsamer
  - **Aufpassen bei**
    - uverschlüsselten Verbindungen – Tor-Knoten (NSA?) können mitlesen
    - Kommunikationspartnern, die einen sowieso kennen

  <++>
- Tails (Freie Software)
  - Abgesichertes Betriebssystem inkl. Tor
  - Leitet *gesamten* Verkehr über Tor
  - Live System = kann direkt von CD gebootet werden hinterlässt keinerlei Spuren am PC

Fahrplan

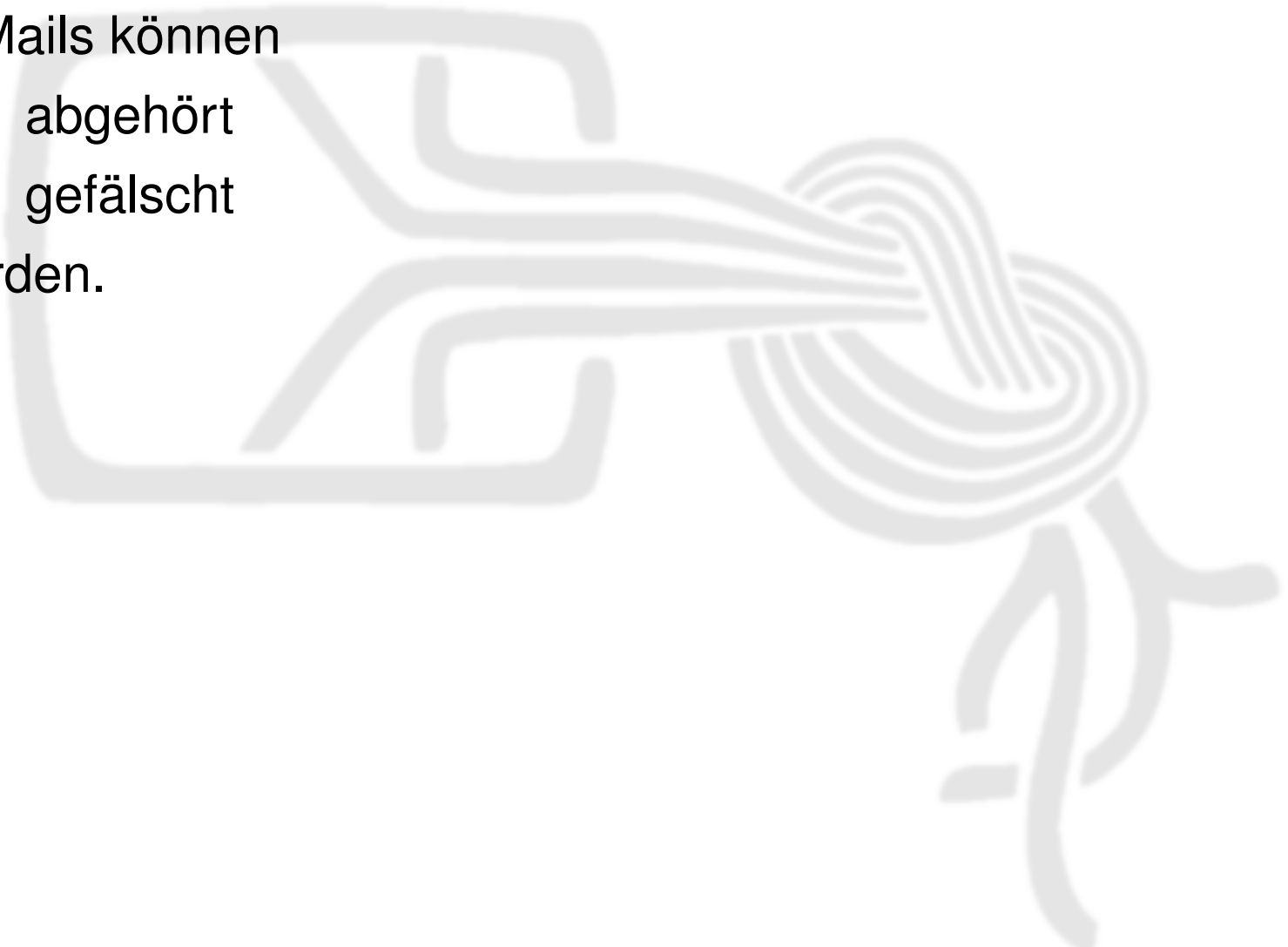


E-Mails: Was soll geschützt werden?

E-Mails können

- abgehört
- gefälscht

werden.

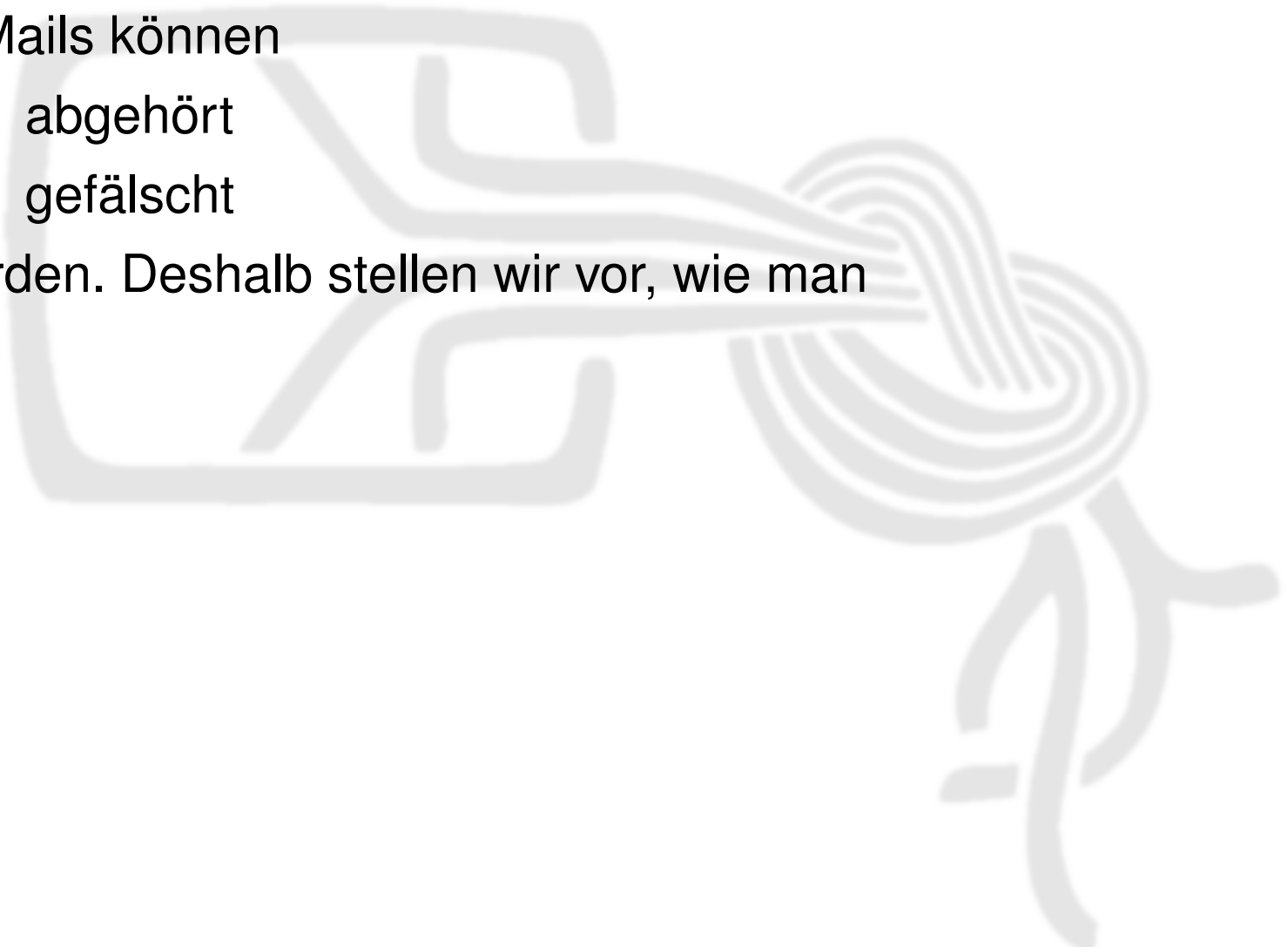


E-Mails: Was soll geschützt werden?

E-Mails können

- abgehört
- gefälscht

werden. Deshalb stellen wir vor, wie man



E-Mails: Was soll geschützt werden?

E-Mails können

- abgehört
- gefälscht

werden. Deshalb stellen wir vor, wie man

- die Vertraulichkeit (das „Briefgeheimnis“) umsetzt
  $\Rightarrow$ Verschlüsselung

E-Mails: Was soll geschützt werden?

E-Mails können

- abgehört
- gefälscht

werden. Deshalb stellen wir vor, wie man

- die Vertraulichkeit (das „Briefgeheimnis“) umsetzt
  $\Rightarrow$ Verschlüsselung
- die Echtheit des Gegenübers sicherstellt
  $\Rightarrow$ Digitale Signatur

E-Mails: Was soll geschützt werden?

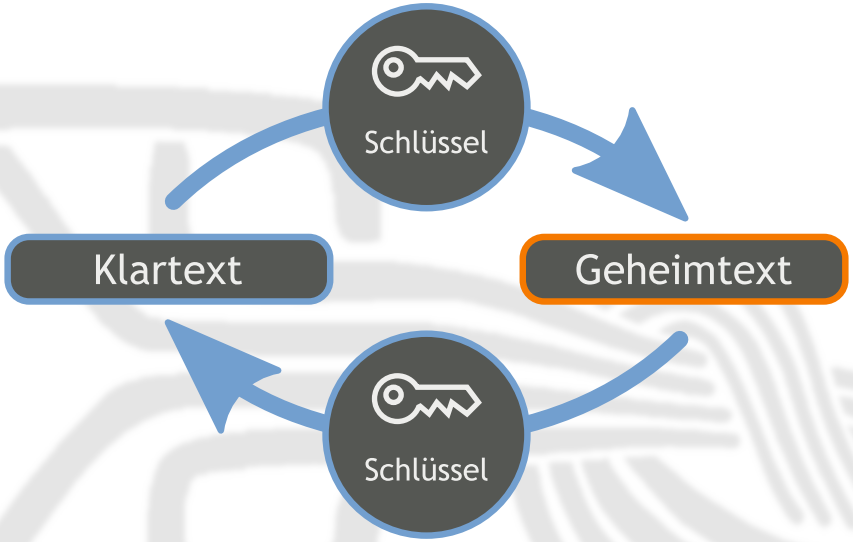
E-Mails können

- abgehört
- gefälscht

werden. Deshalb stellen wir vor, wie man

- die Vertraulichkeit (das „Briefgeheimnis“) umsetzt
  $\Rightarrow$ Verschlüsselung
- die Echtheit des Gegenübers sicherstellt
  $\Rightarrow$ Digitale Signatur
- sicherstellt, dass sein E-Mail-Passwort
  nicht einfach mitgelesen werden kann

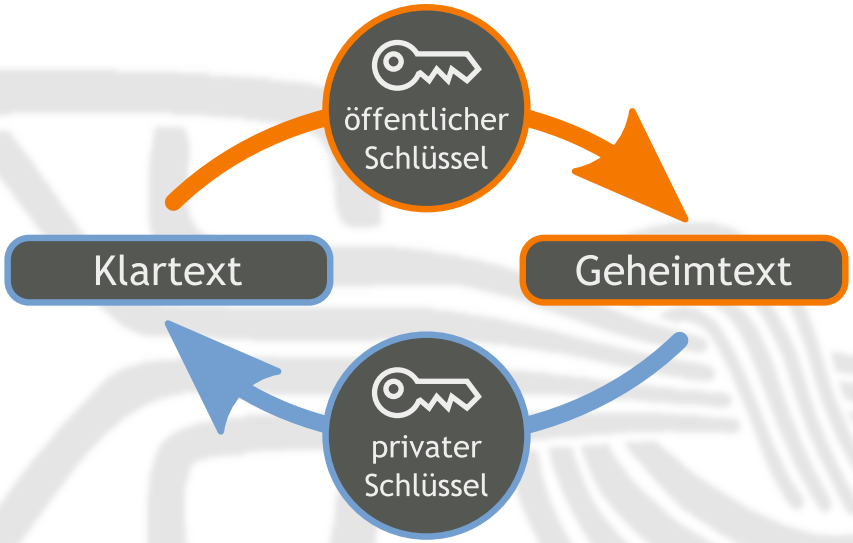
Hintergrundinfo Verschlüsselung
Symmetrische Kryptografie



- Jahrtausende altes Konzept
- *Ein* Schlüssel zum Ver- und Entschlüsseln, den *alle* Beteiligten kennen
- Problem: Schlüsselaustausch
  - Wer den Schlüssel kennt, kommt auch an die Daten
  - Wer den Schlüssel kontrolliert, kontrolliert die Daten
    - Ransomware

Bildquelle: „Symmetrisches Kryptosystem” von Bananenfalter / CC0

Hintergrundinfo Verschlüsselung
Asymmetrische Kryptografie



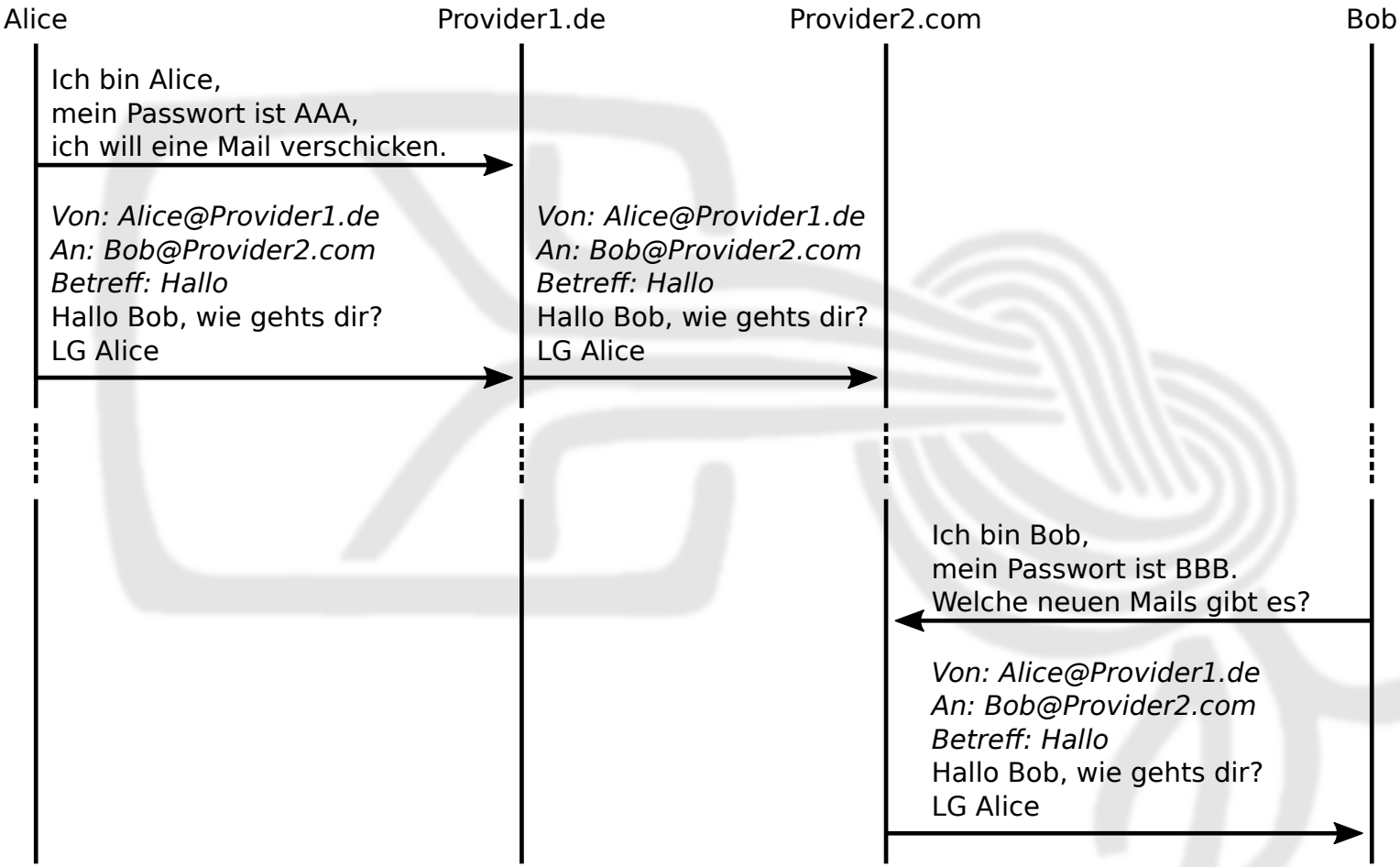
- Prinzip: Schlüssel besteht aus einer *privaten* und einer *öffentlichen* „Hälfte“
  - Öffentlichen Teil darf/muss man weitergeben
  - Privaten Teil muss man unbedingt geheim halten
- Wird verwendet, um vertraulichen Kanal aufzubauen
- Problem weiterhin: Authentizität des öffentlichen Teils

Bildquelle: „Asymmetrisches Kryptosystem mit Verschlüsselung und Entschlüsselung” von Bananenfalter / CC0

- Verschlüsselung
  - Absender *verschlüsselt*
    mit *öffentlichem* Teil des *Gegenübers*
  - Nur Gegenüber
    kann mit *privatem* Gegenstück *entschlüsseln*
- Digitale Signatur
  - Absender unterschreibt mit *eigenem privaten* Teil
  - Jeder kann mit *öffentlichem* Gegenstück *überprüfen*

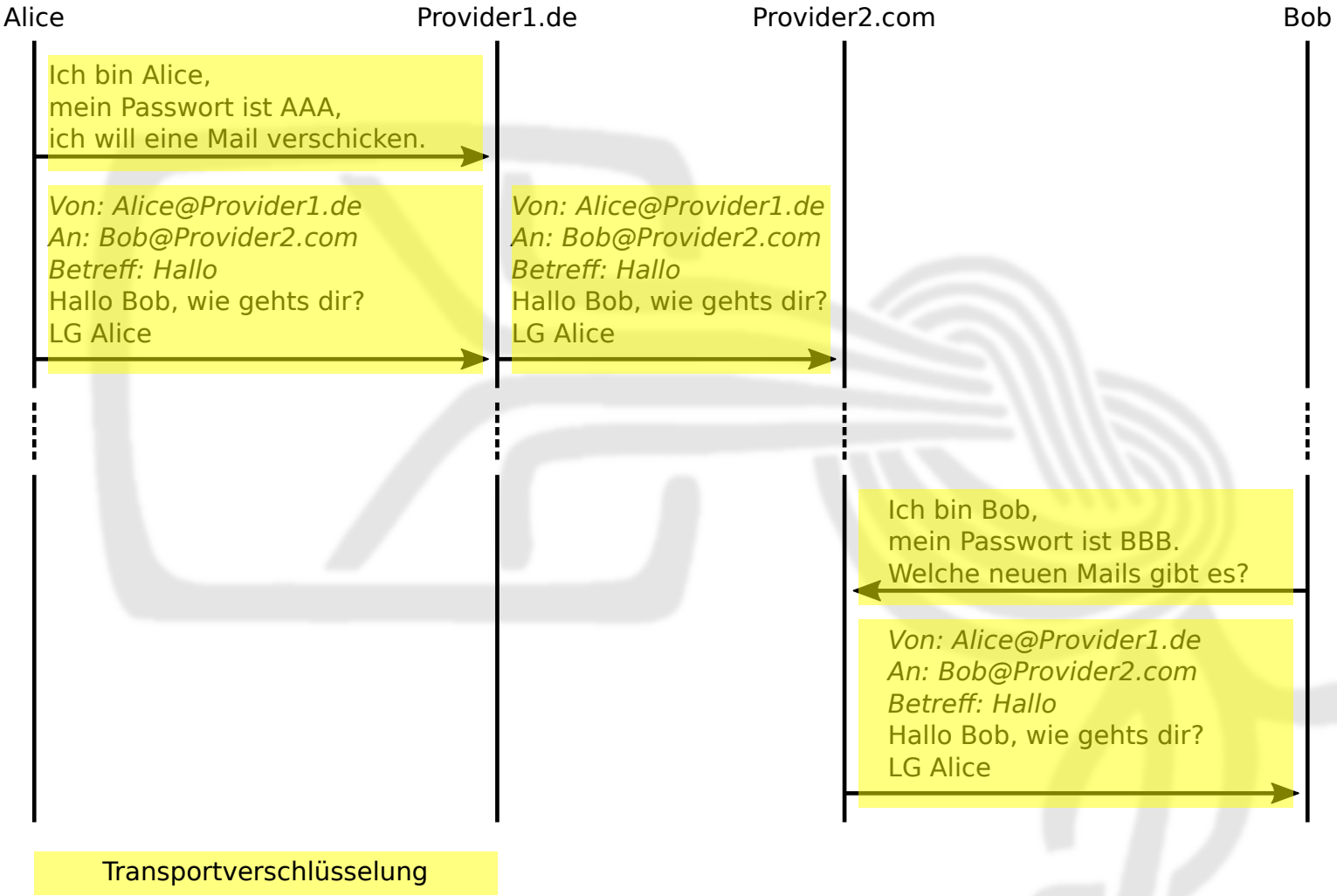
Es ist mathematisch komplex und benötigt Jahrtausende,
um aus einer Signatur oder dem öffentlichen Teil
den privaten Teil zu berechnen

E-Mail
Funktionsweise



E-Mail

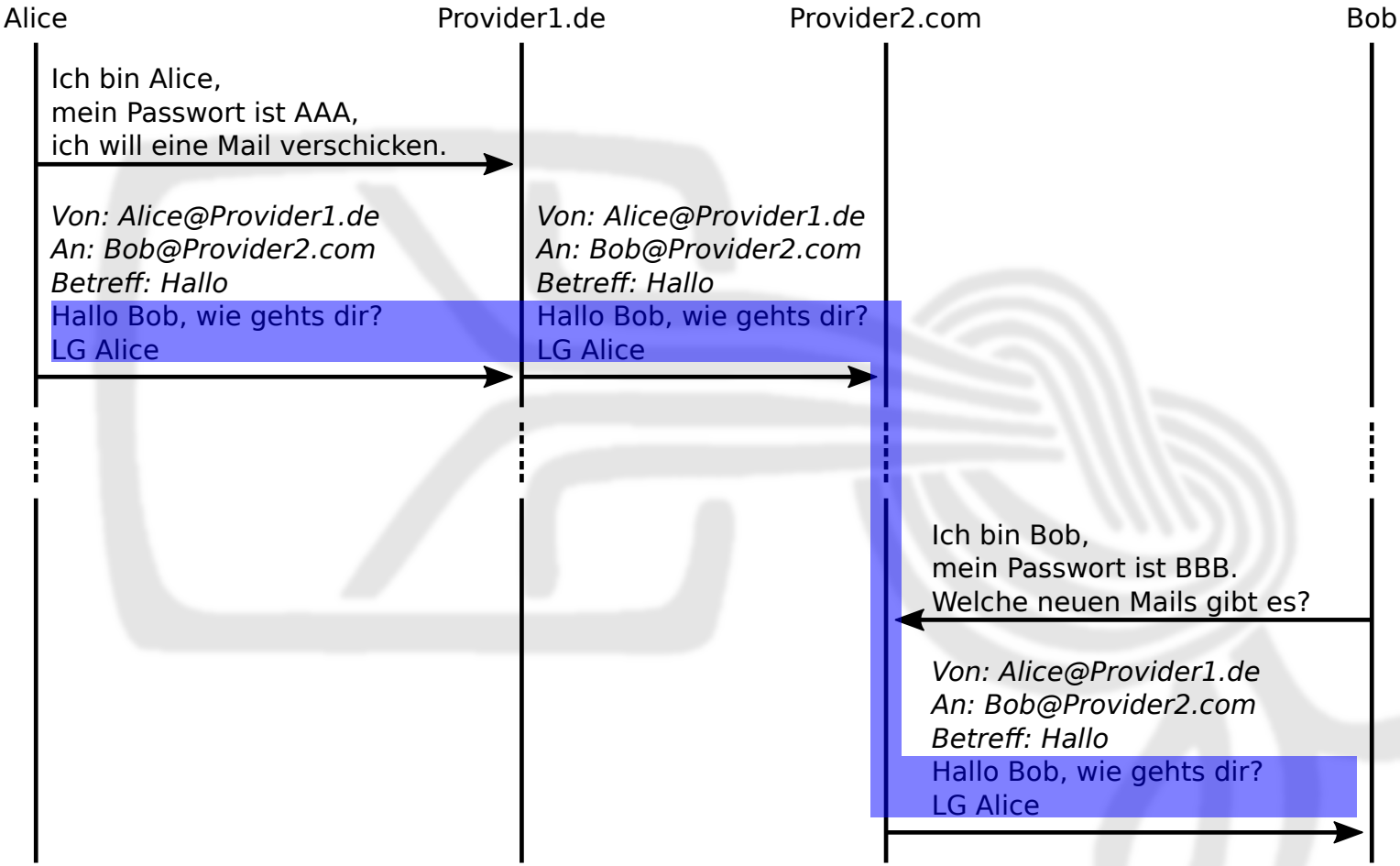
Transportverschlüsselung (SSL/TLS bzw. STARTTLS)



- muss von den Mailanbietern unterstützt werden
- Konfiguration des Mailprogramms überprüfen!

E-Mail

Ende-zu-Ende-Verschlüsselung (OpenPGP, S/MIME)

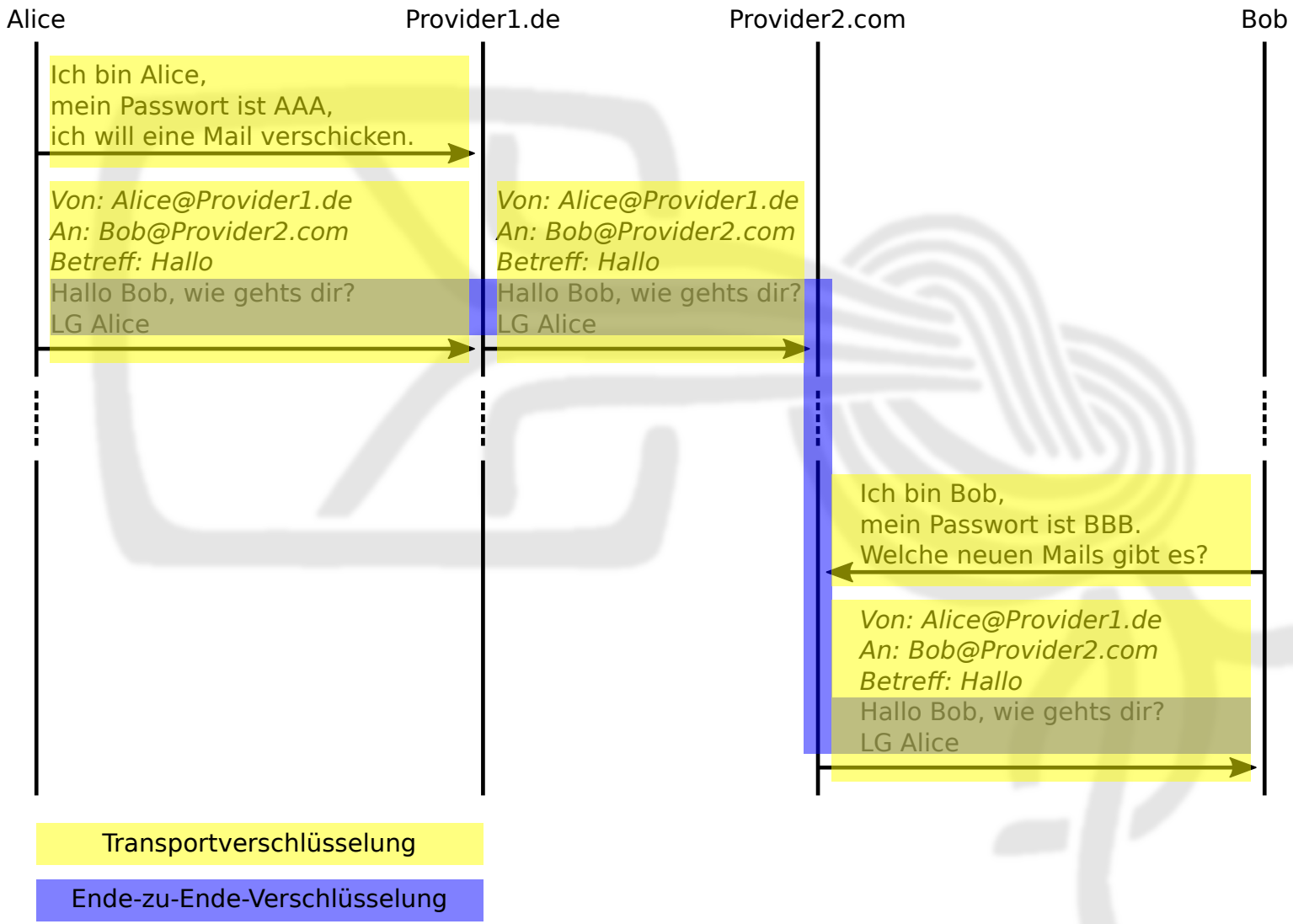


Ende-zu-Ende-Verschlüsselung

- unabhängig vom Mailanbieter möglich
- benötigt Zusatzsoftware und Schlüssel bei beiden Kommunikationspartnern

E-Mail

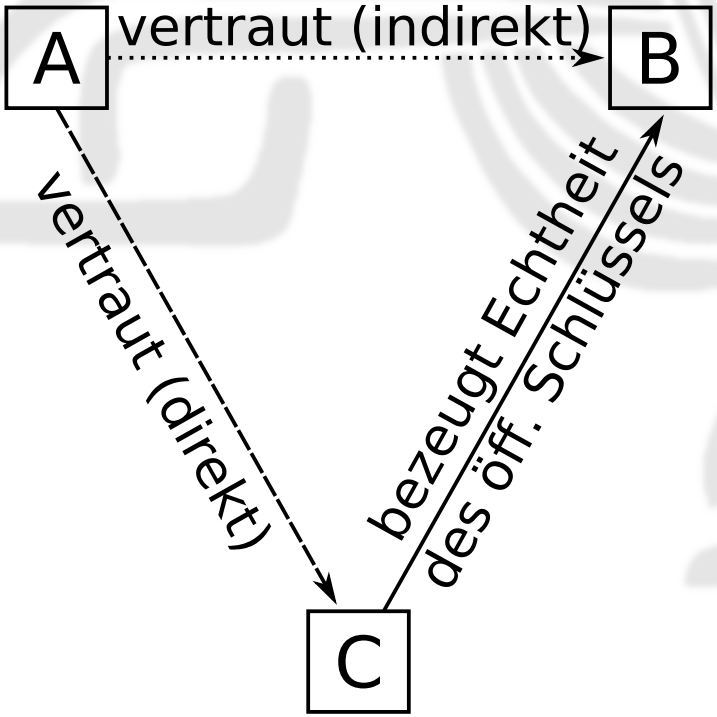
Kombination Transport- und Ende-zu-Ende-Verschlüsselung



Authentizität öffentlicher Schlüssel

Was, wenn A eine Nachricht an B schicken will,
aber den öffentlichen Schlüssel von B nicht kennt?

1. Im “Telefonbuch” nach dem Schlüssel suchen
2. Echtheit mit Hilfe eines *vertrauenswürdigen Dritten* C überprüfen



Wie stellt man Vertrauen in öffentliche Schlüssel her?

- S/MIME – Hierarchischer Vertrauensansatz
  - hier nicht behandelt
- OpenPGP – Dezentraler Vertrauensansatz
  - jeder kann festlegen, wem er vertraut
    - er kann die Echtheit eines Schlüssels
      z.B. bei einem persönlichen Treffen überprüfen
  - jeder *kann* sein Vertrauensnetz veröffentlichen (Web-of-Trust)
    - Vorteil: Man kann “Freunden von Freunden” vertrauen
    - Nachteil: Beziehungen zwischen Menschen öffentlich
      Aber: Facebook sagt da viel mehr aus

Welche Software benötigt man?

OpenPGP Backend

Macht die eigentliche Ver-/Entschlüsselung & Signatur

Linux:	Windows:	Android:	Mac:
on-board	GPG4Win	OpenKeychain	GPGTools[a]

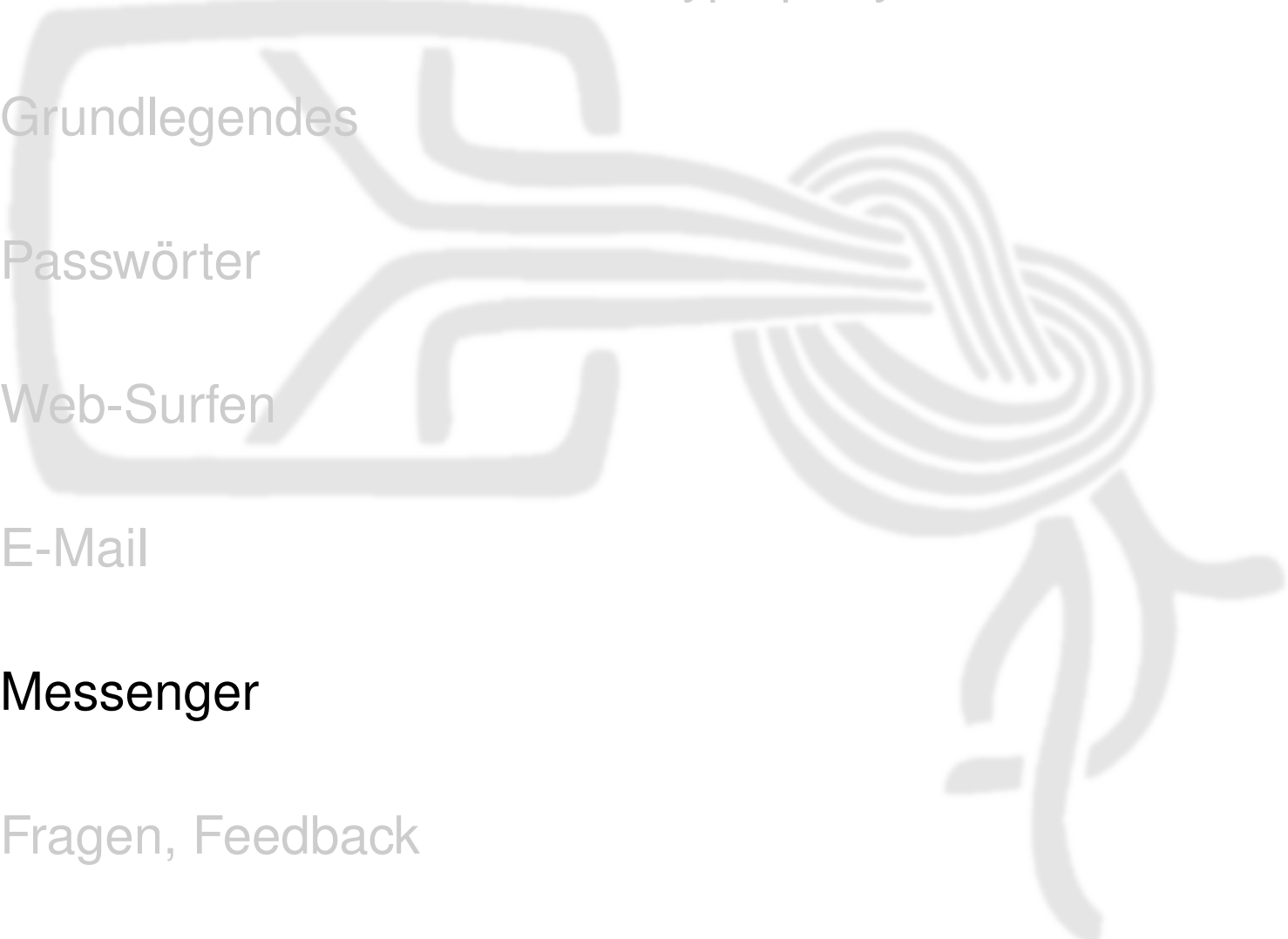
[a] kommerziell

Plug-In fürs Mailprogramm

Grafische Oberfläche, leichtere Schlüsselverwaltung, etc.

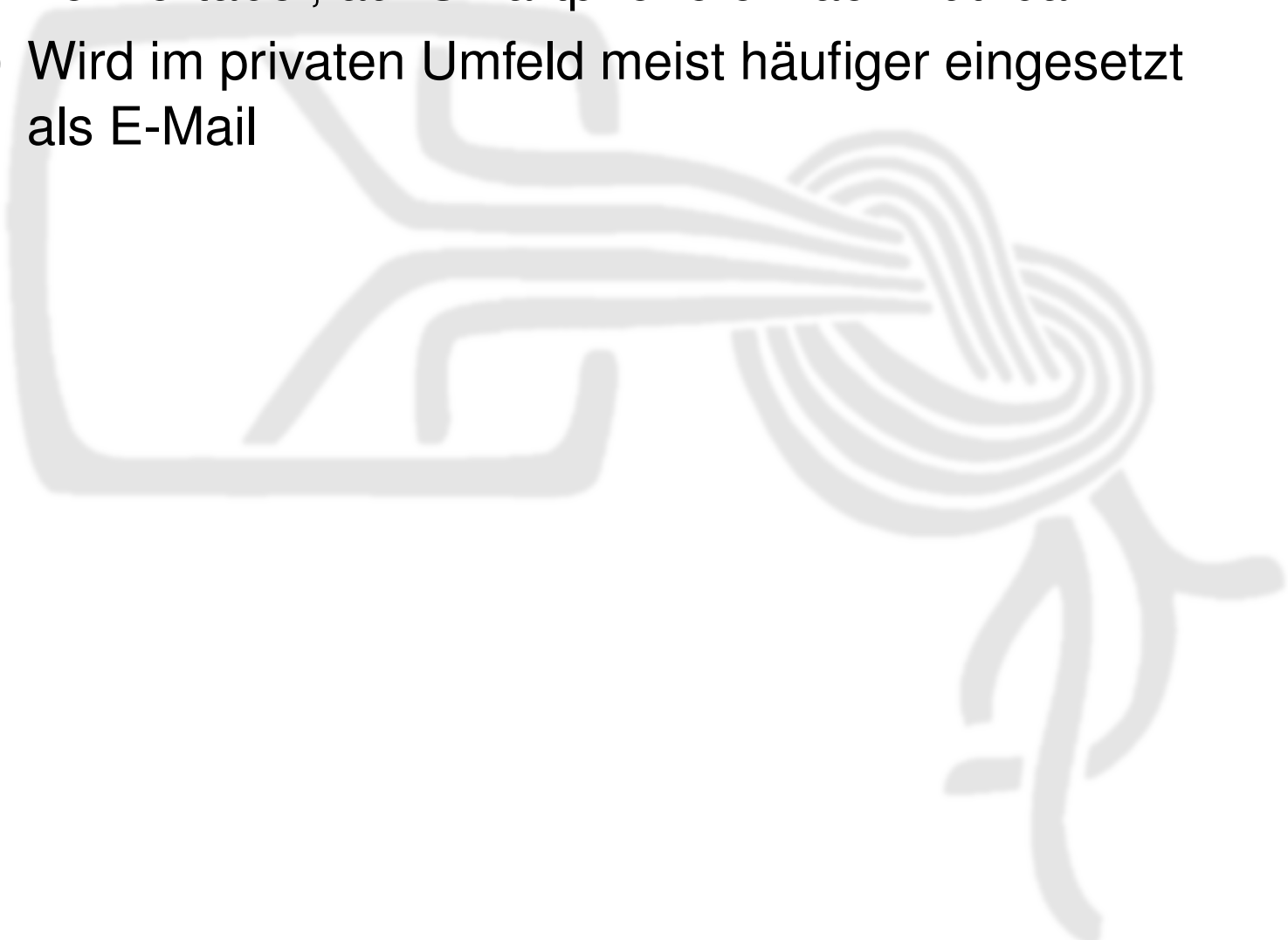
Thunderbird:	Outlook:	K9-Mail:	Apple Mail:
Enigmail	GPG4Win	*integriert*	GPGTools

Fahrplan



Motivation

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail



Motivation

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

Bestandsaufnahme

Wer benutzt

- WhatsApp

Motivation

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

Bestandsaufnahme

Wer benutzt

- WhatsApp
- Telegram

Motivation

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

Bestandsaufnahme

Wer benutzt

- WhatsApp
- Telegram
- Threema

Motivation

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

Bestandsaufnahme

Wer benutzt

- WhatsApp
- Telegram
- Threema
- Signal

Motivation

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

Bestandsaufnahme

Wer benutzt

- WhatsApp
- Telegram
- Threema
- Signal
- Jabber

Motivation

- Komfortabel, auf Smartphone einfach nutzbar
- Wird im privaten Umfeld meist häufiger eingesetzt als E-Mail

Bestandsaufnahme

Wer benutzt

- WhatsApp
- Telegram
- Threema
- Signal
- Jabber
- Matrix

Überblick

- Geschlossene Systeme: WhatsApp & Co
  - App-Entwickler
    ist Dienstanbieter
    und Herr über die “technische Sprache” (das Protokoll)
  - Auswahl eines Dienstes
    bestimmt erreichbaren Personenkreis
  - meist Closed Source
- Offene Systeme (z.B. Jabber/XMPP, Matrix)
  - App-Entwickler, Dienstanbieter und
    Protokoll-Standardisierer sind unterschiedliche Personen
  - App und Anbieter frei wählbar
  - meist Open Source

WhatsApp

Vor- und Nachteile

+ Angeblich sehr gute Crypto (von Signal eingekauft)
+ Verwendbar ohne Google Play Services
- Closed Source
- Anbieter erhält vollständiges Telefonbuch (nicht nur WhatsApp-Kontakte)
- Metadatenanalyse, -weitergabe an Facebook

Tipps

- Ab Android 6 und bei iOS kann man für WhatsApp den Zugang zum Telefonbuch sperren
- Android 8 Dual Messenger erlaubt selektive Freigabe von Kontakten
  nicht getestet, nur Samsung(?)

Telegram

Vor- und Nachteile

+ „Sichere Chats“ bieten ausreichende Sicherheit
- Chats nicht standardmäßig verschlüsselt
- Anbieter erhält vollständiges Telefonbuch (nicht nur Telegram-Kontakte)
- „Standard-Chats“ werden im Klartext beim Anbieter gespeichert

Threema

Vor- und Nachteile

+ Chats hinreichend gut verschlüsselt
  (aber nicht gut überprüfbar, da nicht quelloffen)
+ Synchronisation des Telefonbuchs optional
+ Überprüfung der Schlüssel über QR-Code
o kostenpflichtig
- nicht quelloffen

Signal

Vor- und Nachteile

+ Chats standardmäßig sehr gut verschlüsselt
+ Überprüfung der Schlüssel über QR-Code
- Anbieter erhält komplettes Telefonbuch (nicht nur Signal Kontakte)

Jabber/XMPP

Vor- und Nachteile

+ Offenes System: Anbieter und App frei wählbar
+ Verschlüsselung möglich (OTR oder OMEMO)
+ keine Telefonbuch-Synchronisation vorgesehen
- Crypto nicht ganz so nutzerfreundlich
  wie bei kommerziellen Anbietern
  (aber dafür sind wir ja alle hier :-)

- Apps: Conversations, pidgin, gajim, ...
- Anbieter: Unis, Hackerspaces, CCC, jabber.org, ...

Matrix

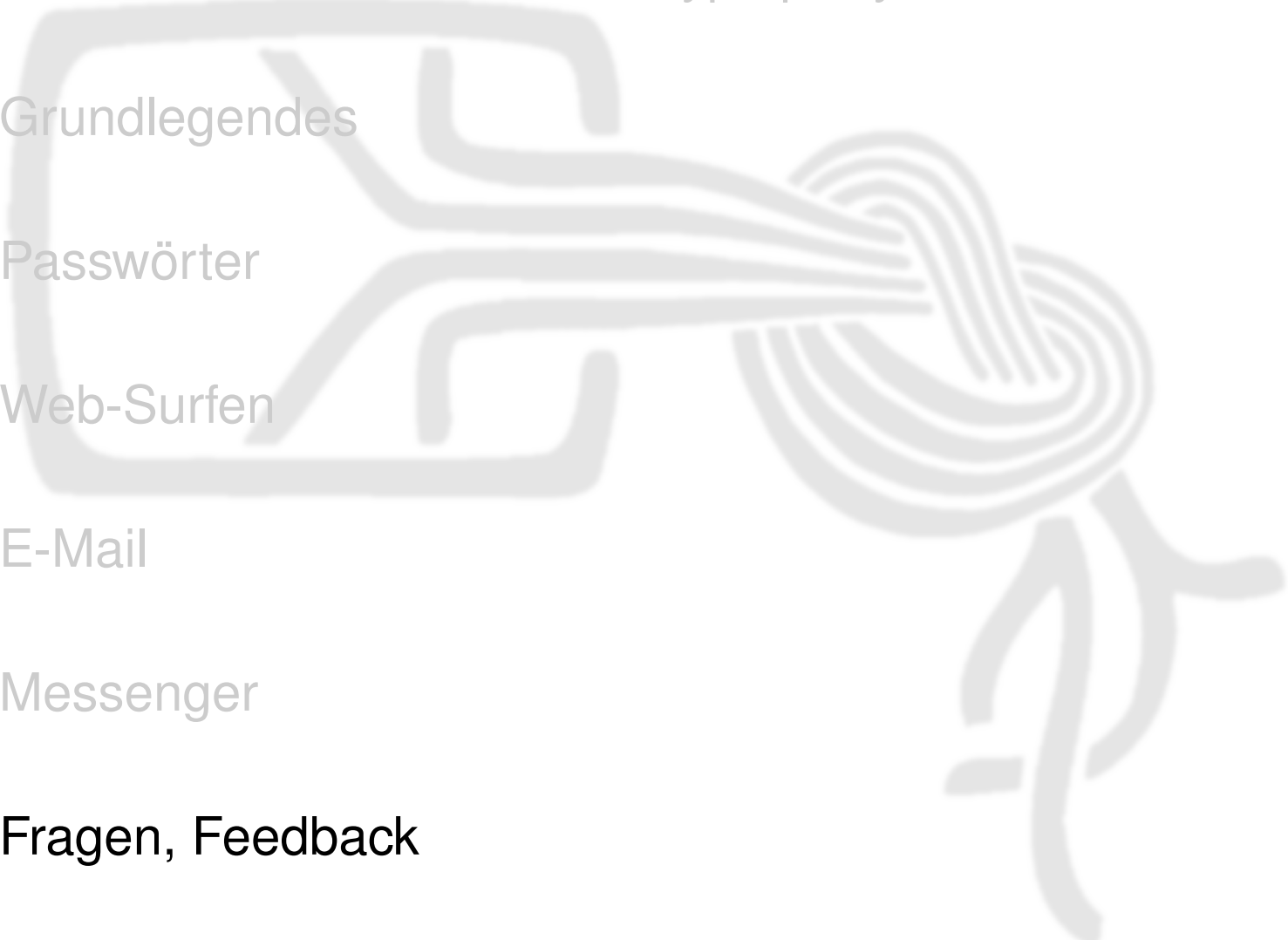
Vor- und Nachteile

+ Offenes System: Anbieter frei wählbar
+ Verschlüsselung möglich
+ Telefonbuch-Synchronisation nicht zwingend
+ Anbindung an Drittsysteme möglich (IRC, Skype, . . .)
- Hintergrund/Historie der Entwickler umstritten

Zusammenfassung

- Viele beliebte Messenger sind geschlossene Systeme
- darauf achten, womit Anbieter sein Geld verdient
- Wer auf bestimmten Messenger nicht verzichten kann: Zugriff auf Kontakte verbieten!

Fahrplan



Fragen, Feedback, ...

- Her damit!
- Fragen an alle Helfer (bitte gebt Euch zu erkennen :-)
- Links
  - `https://www.prism-break.org`
  - `https://muc.pads.ccc.de/cryptoparty`