Piratenpartei

Ennepe-Ruhr

CryptoParty

digitale Selbstverteidigung

CryptoParty

digitale Selbstverteidigung

PIRATENPARTEI
Ennepe-Ruhr-Kreis

https://piraten-en.de

PIRATEN FRAKTION WITTEN

https://piraten-witten.de

ANKERPLATZ

PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

- **Stefan Borggraefe**
  - Software-Entwickler und Systemadministrator
  - Vorsitzender Piratenpartei Kreisverband Ennepe-Ruhr
  - Ratsmitglied in Witten
  - stefan@piraten-en.de
  - Twitter: @BorgTenOfNine

PIRATEN WÄHLEN

Wer sollte verschlüsseln?

- Firmen (Geschäftsgeheimnisse)
- Anwälte, Geistliche, Ärzte, …
- Journalisten (Quellenschutz!)
- Politische Aktivisten
- Alle, die nicht ihr Tagebuch offen herumliegen lassen würden.
- Alle! Aus Solidarität!

CryptoParty

digitale Selbstverteidigung

Lernziele heute

- Einige wenige theoretische Grundlagen
- E-Mails verschlüsseln
- Anonym surfen
- Tipps zur Verkleinerung des Datenschattens
- Sensibilisierung für das Thema Überwachung

Sicherheit und Vertrauen

- Absolute Sicherheit gibt es nicht
  - Es geht um die Minimierung von Risiken
- Informiere Dich!
  - Wie finanzieren sich Dienste im Internet?
  - Wer ist das Produkt? Wo kommt das Geld her?
- Rechne mit Datenpannen!
- Freie Software lässt sich besser prüfen!

CryptoParty

digitale Selbstverteidigung

Freie Software

- Die Freiheit, das Programm für jeden Zweck auszuführen.
- Die Freiheit, die Funktionsweise des Programms zu untersuchen.
- Die Freiheit, das Programm weiter zu verbreiten und damit seinen Mitmenschen zu helfen.
- Die Freiheit, das Programm zu verbessern und diese Verbesserungen der Öffentlichkeit freizugeben, damit die gesamte Gemeinschaft davon profitiert

Nicht-freie Software =
proprietäre Software

CryptoParty

digitale Selbstverteidigung

Drei wichtige Ziele der Kryptografie

- Vertraulichkeit

PIRATEN WÄHLEN

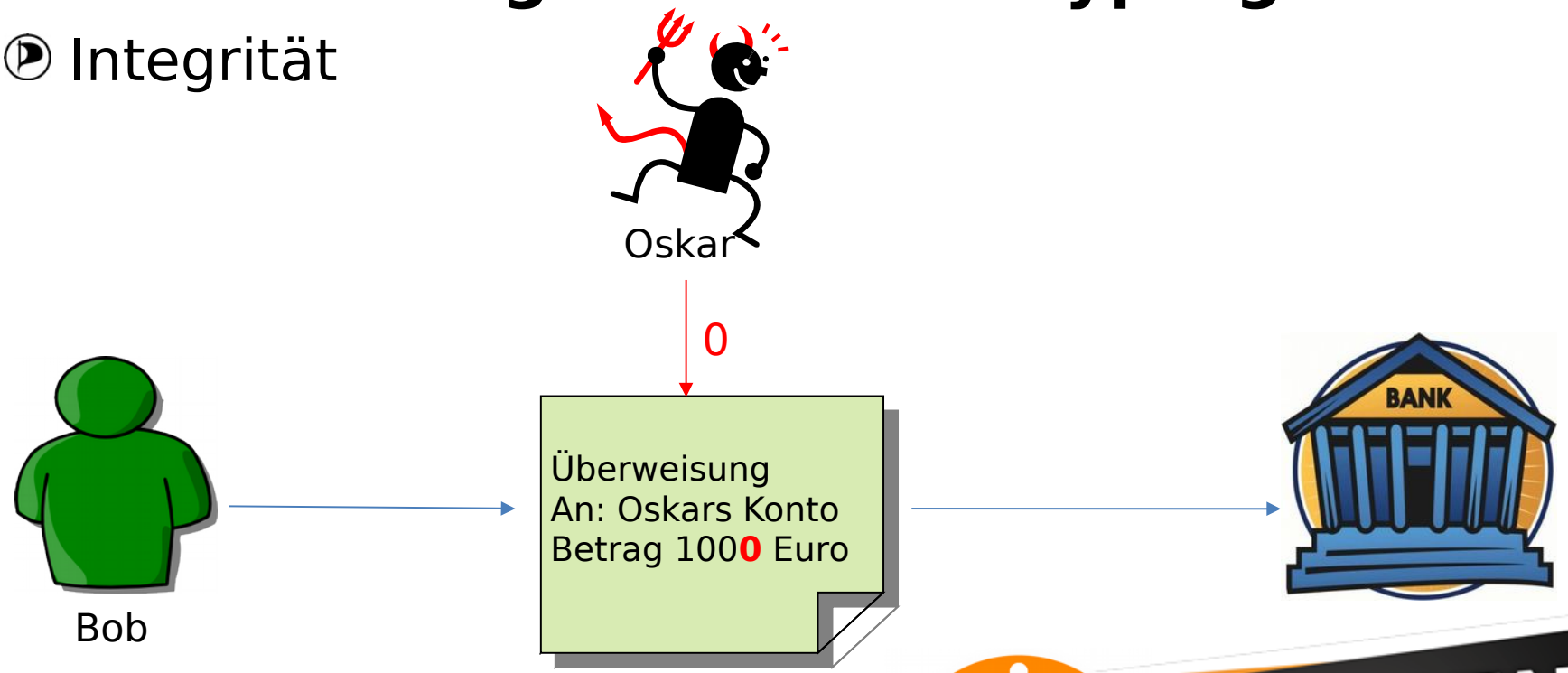
Drei wichtige Ziele der Kryptografie

- Authentizität

PIRATEN
WÄHLEN

Drei wichtige Ziele der Kryptografie

- Integrität



PIRATEN
WÄHLEN

CryptoParty

digitale Selbstverteidigung

Verschlüsselung in der Geschichte

Bild: CC-BY-SA 3.0 Eivind Lindbråten

Skytale

Erfunden: ~ 700 v. Chr.

Transpositionsverfahren

PIRATEN WÄHLEN

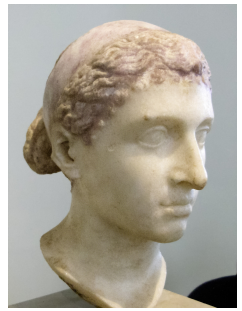
CryptoParty

digitale Selbstverteidigung

Caesar Chiffre

Monoalphabetische Substitution

Statistische
Häufigkeitsanalyse



A	B	C	D	[…]
Q	*F*	*H*	*B*	*[…]*

CryptoParty

digitale Selbstverteidigung

Enigma

Polyalphabetische Subsitution

PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

Symmetrische vs. asymmetrische Kryptosysteme

symmetrisch

- Alle Teilnehmer verwenden einen gemeinsames Geheimnis
- Problem: Schlüsselaustausch

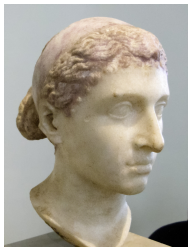
asymmetrisch

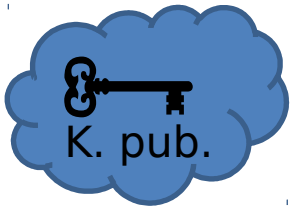
- Erfunden in den 70ern
- Prinzip: Private-Public-Key
- Vorteil: Schlüsselaustausch vereinfacht (z.B. durch Keyserver)

CryptoParty

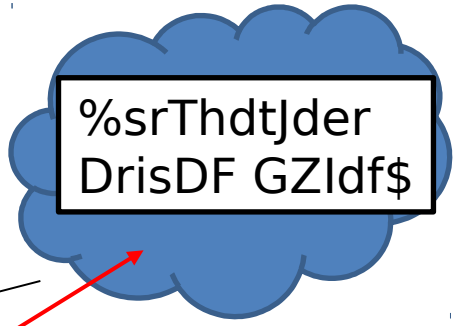
digitale Selbstverteidigung

Symmetrische vs. asymmetrische Verschlüsselung





„Ich liebe dich!
Dein Caesar“



„Ich liebe dich!
Dein Caesar“

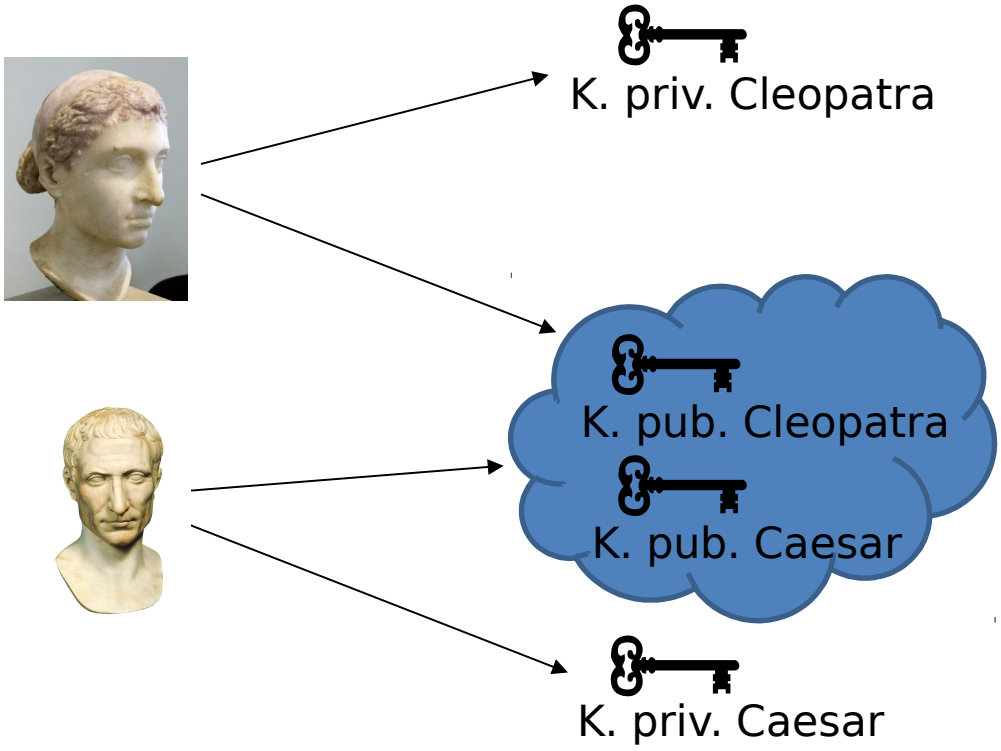
Keine Chance

PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

Asymmetrische Verschlüsselung

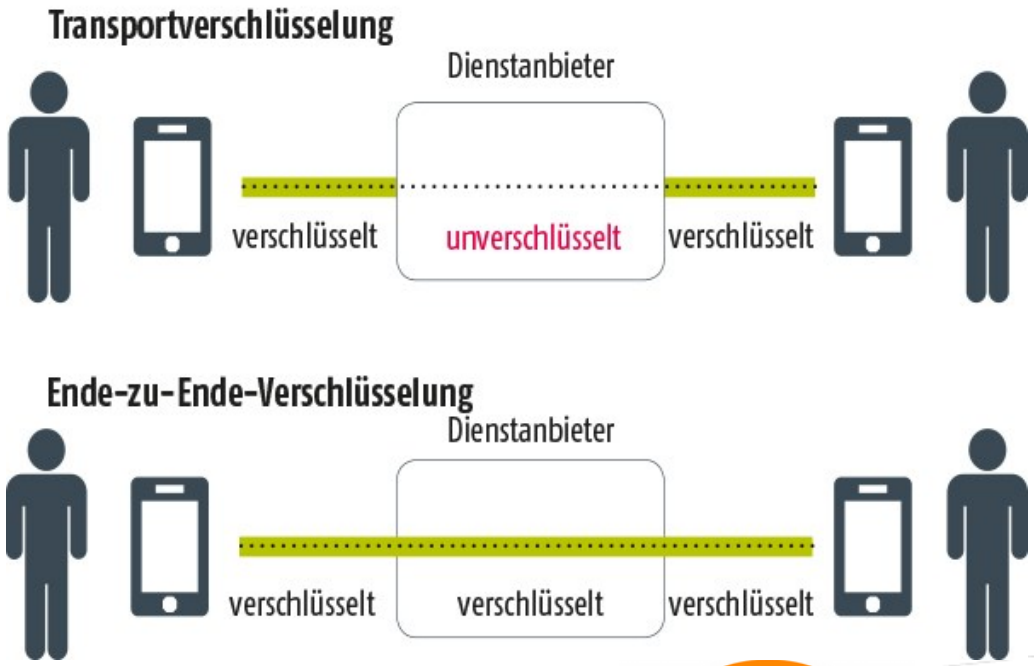


PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

Transport- vs. Ende-zu-Ende-Verschlüsselung



PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

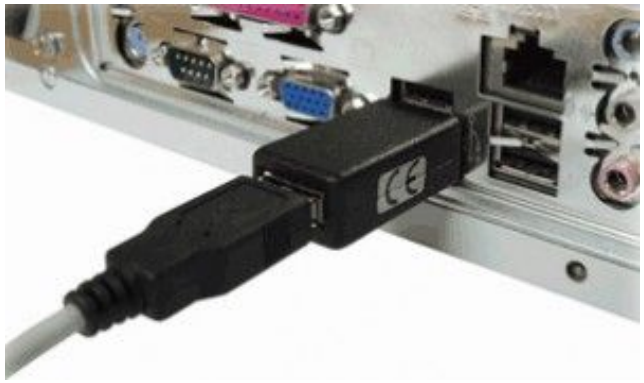
Live Demo

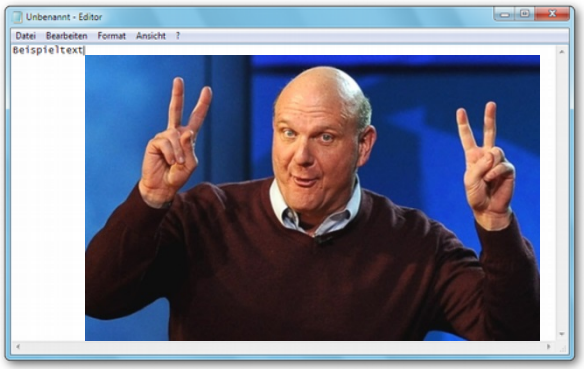
- Thunderbird, GnuPG & Enigmail

CryptoParty

digitale Selbstverteidigung

Mögliche Angriffe gegen Verschlüsselung





PIRATEN WÄHLEN

Empfehlenswerte Messenger

- Signal Secure Messenger
- Wire
- Threema

PIRATEN WÄHLEN

Messenger – WhatsApp

- Inzwischen auch Ende-zu-Ende verschlüsselt
  - Signal-Protokoll
  - Aber proprietär
- Gehört aber zum Facebook-Konzern
  - Monetarisierung der Meta-Daten

PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

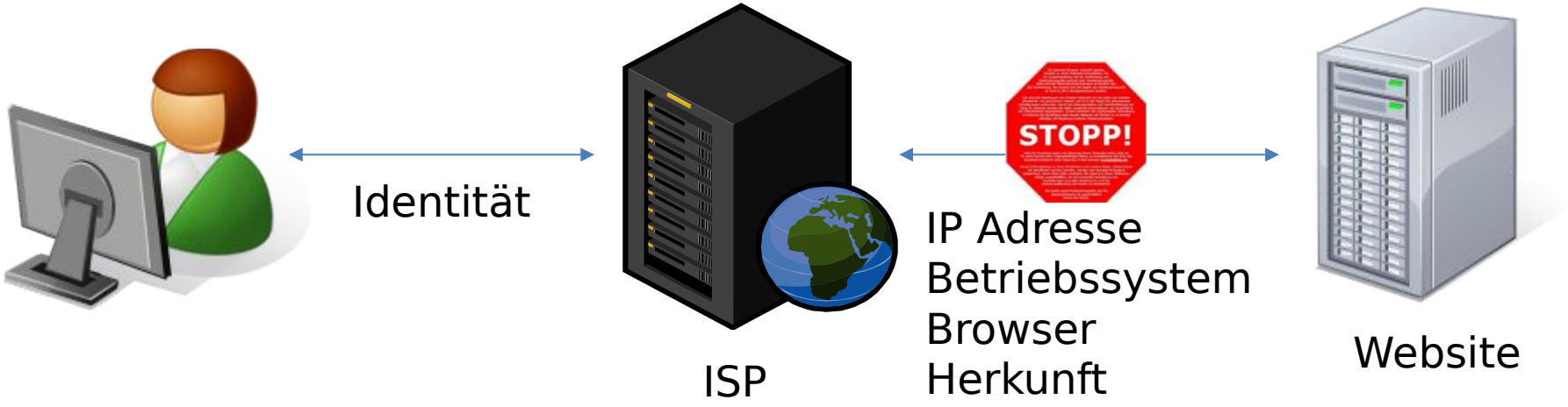
Empfehlenswerte Browser-Addons

- HTTPS-Everywhere
- Privacy Badger
- uBlock Origin

CryptoParty

digitale Selbstverteidigung

Tor

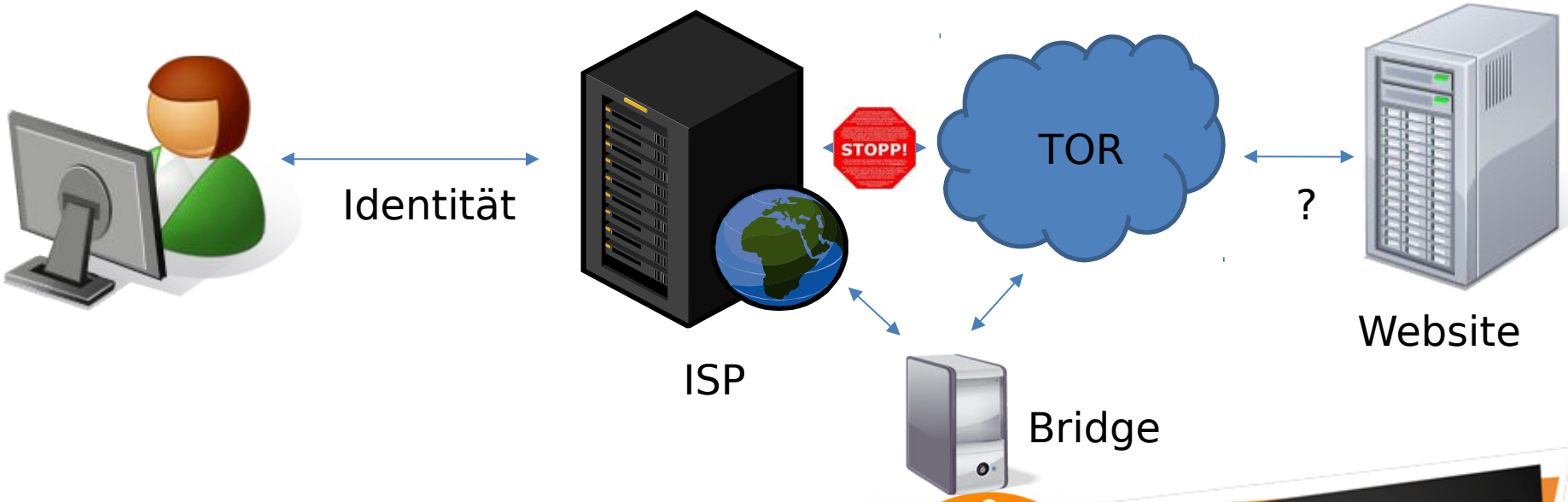


PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

Tor

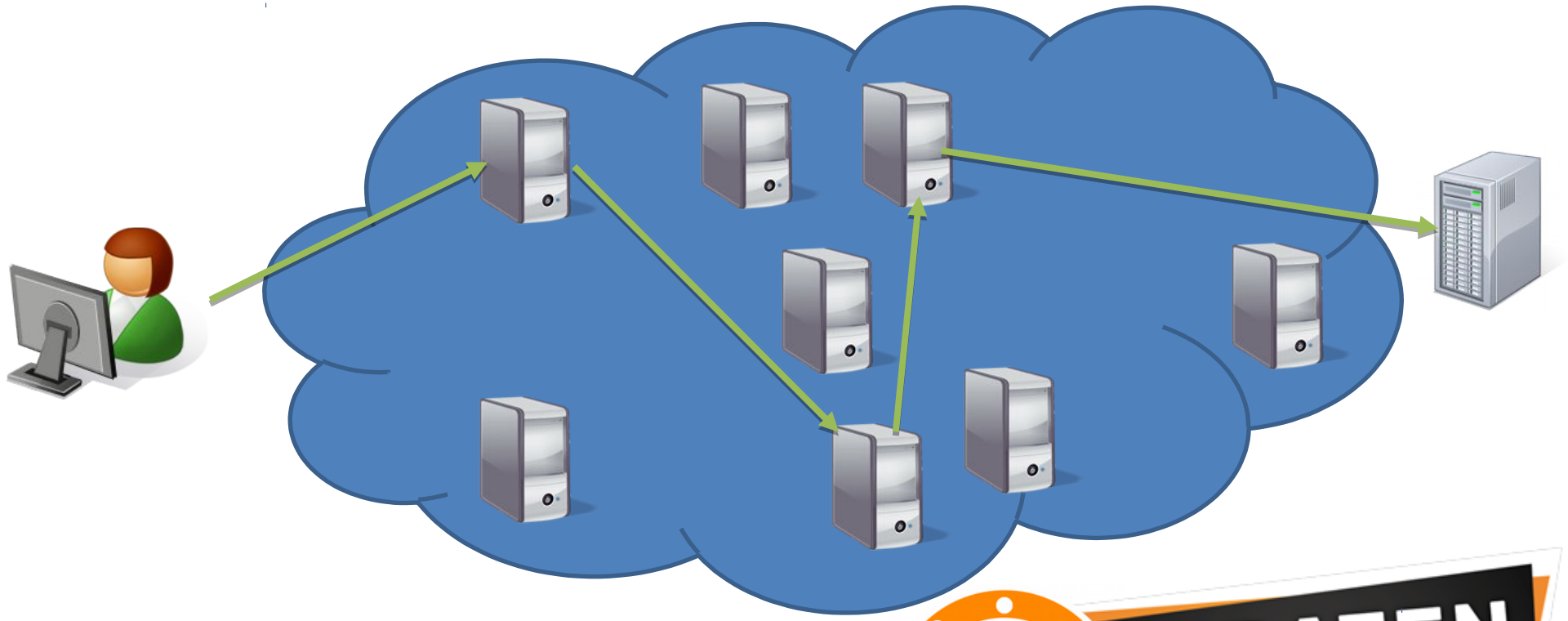


PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

Tor



PIRATEN WÄHLEN

Live Demos

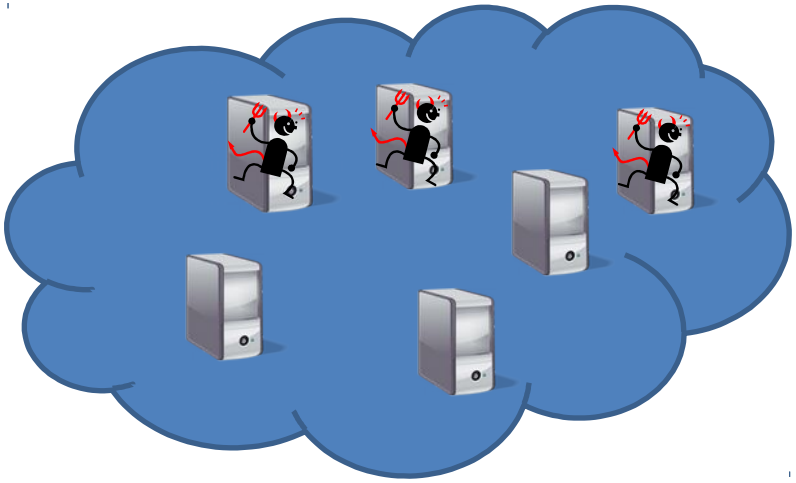
- Tor
  - https://www.torproject.org/projects/torbrowser.html
- Tails
  - https://tails.boum.org/

PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

Angriffe gegen Tor



PIRATEN WÄHLEN

CryptoParty

digitale Selbstverteidigung

Sichere Dropbox-Alternativen

Nextcloud

SpiderOak

PIRATEN WÄHLEN

Fazit

- Absolute Sicherheit gibt es nicht
- Mit etwas Aufwand kann man seine Privatsphäre dennoch adäquat schützen

PIRATEN WÄHLEN