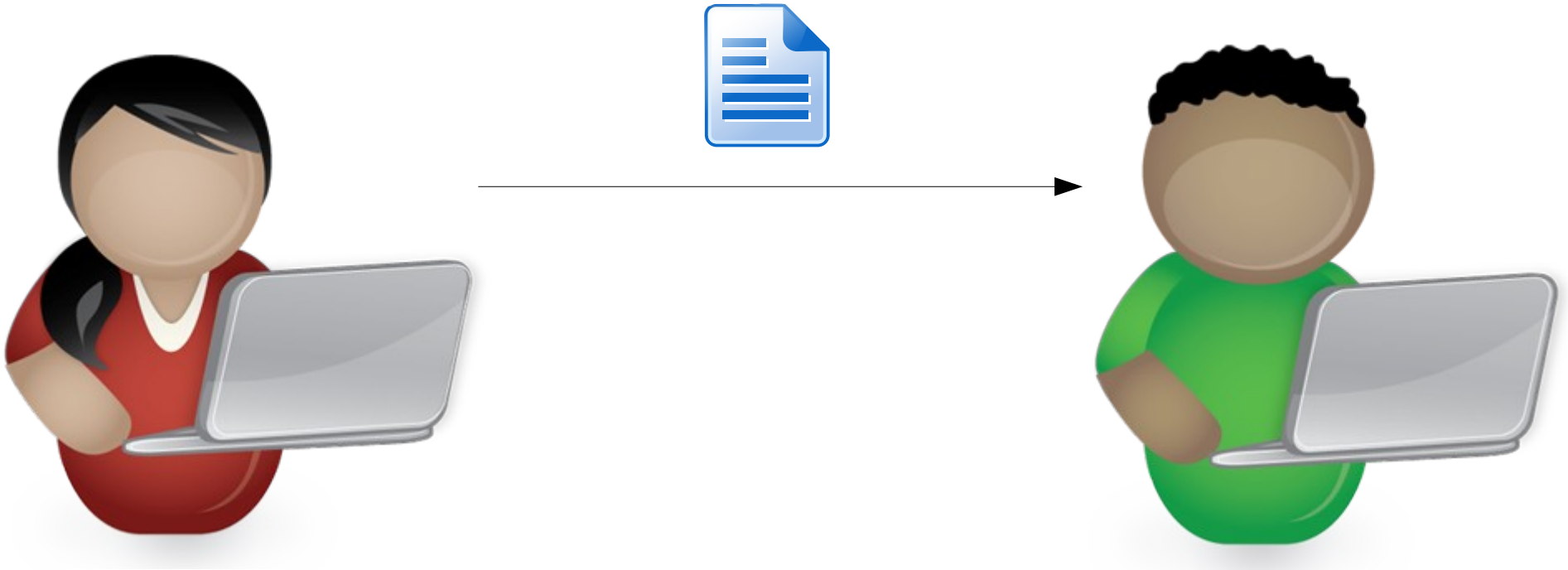
Verschlüsselte Kommunikation

Panda & vmann

Inhalt

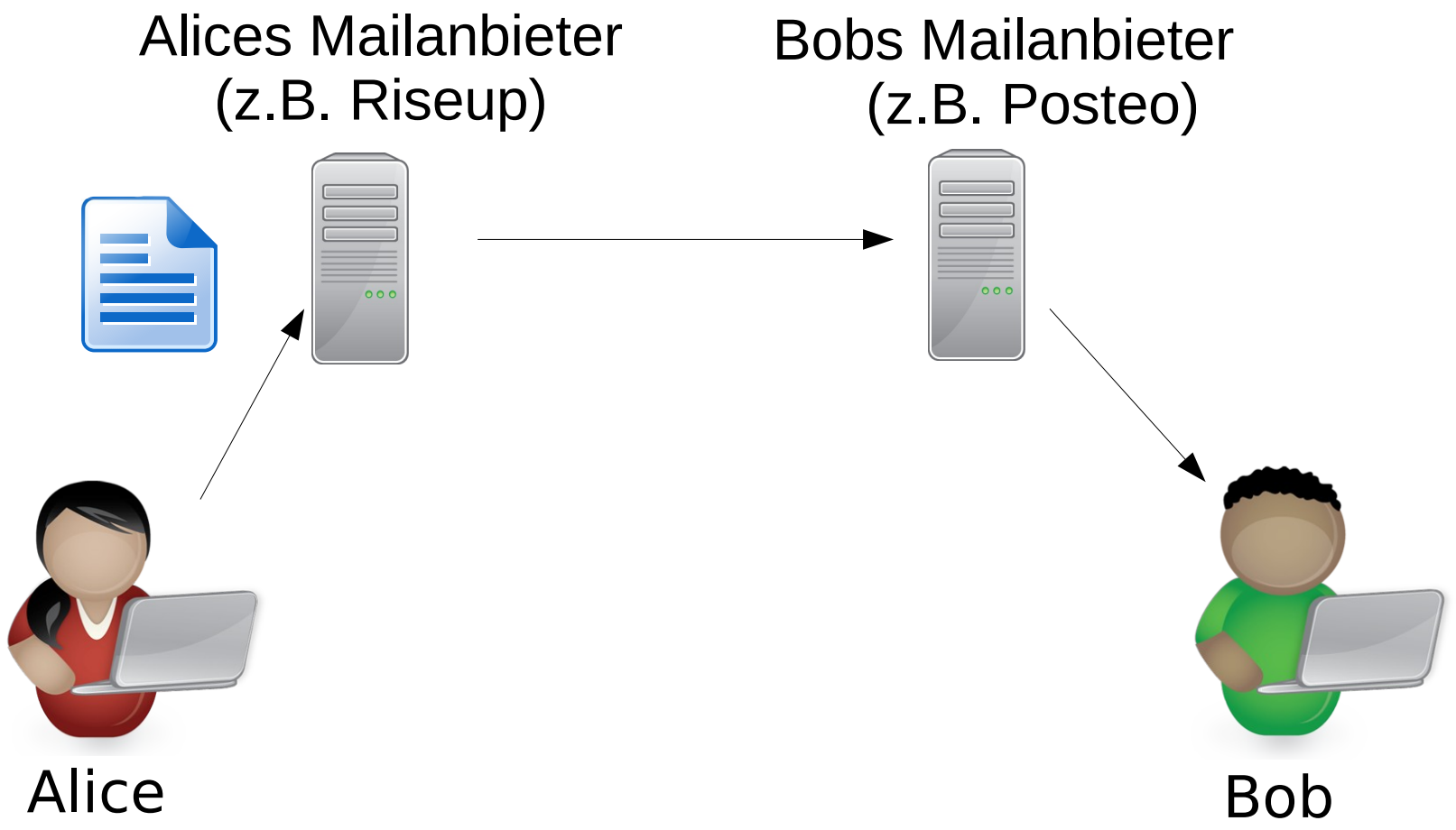
- Verschlüsselung in Netzwerken – warum?
- Verschlüsselung 101
- Ende-zu-Ende-Verschlüsselung
  - Sichere Nutzung
  - Forward Secrecy
  - Grenzen

Kommunikation im Internet



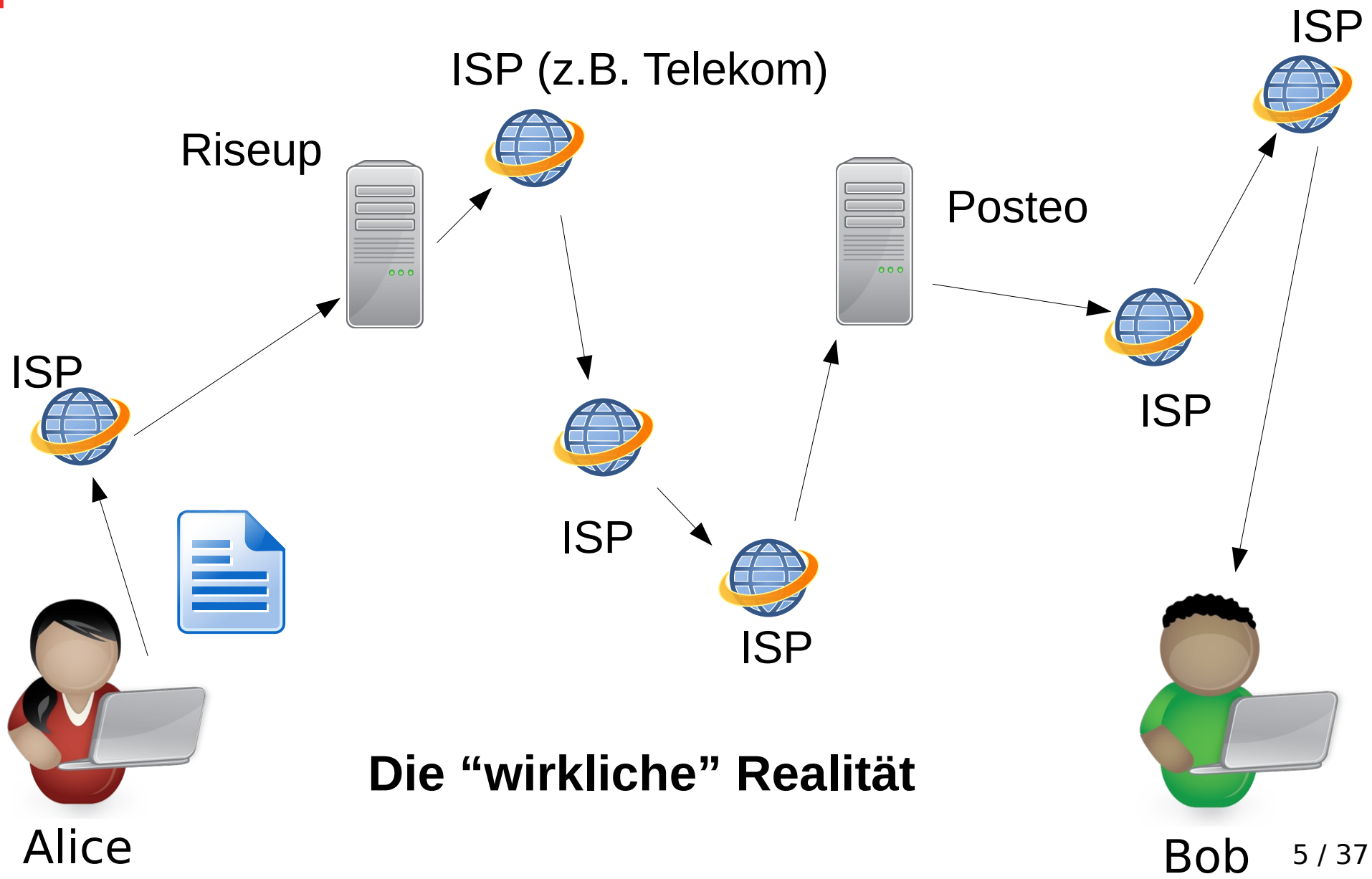
Die Idee

Kommunikation im Internet



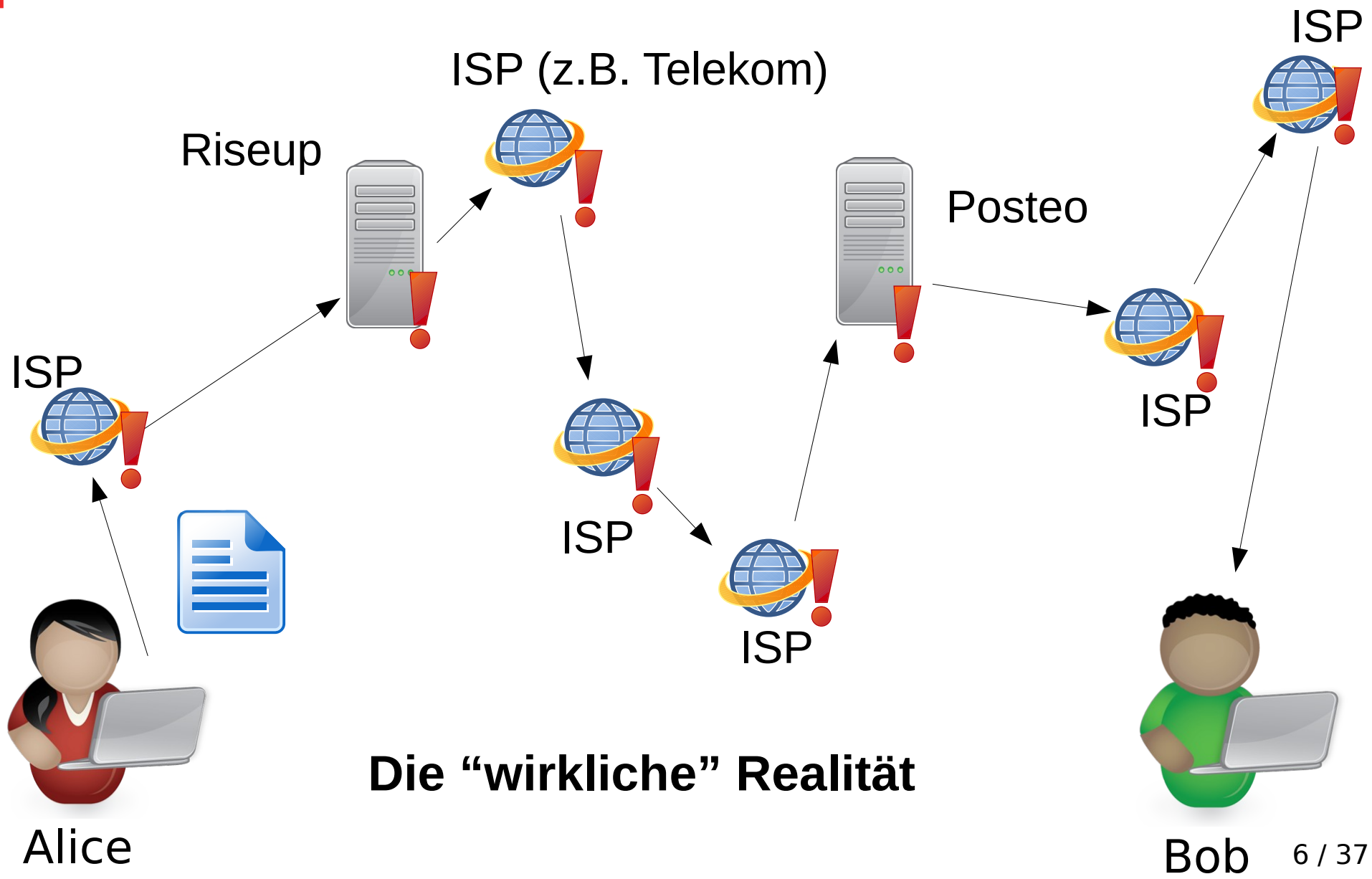
Die Realität

Kommunikation im Internet



Die “wirkliche” Realität

Kommunikation im Internet



Die “wirkliche” Realität

“Lawful” Interception

- Artikel 10 Gesetz
  - BND: “strategische Telekommunikationsüberwachung”
  - Verfassungsschutz
  - MAD
- StPO §100a ff.:
  - BKA: “Telekommunikationsüberwachung”

heise online › News › 05/2018 › **Gerichtsurteil: BND darf weiterhin Internet-Knoten De-CIX anzapfen**

Gerichtsurteil: BND darf weiterhin Internet-Knoten De-CIX anzapfen

ISP

Der Bundesnachrichtendienst kann weiterhin am Internet-Knoten De-CIX anlasslos Daten abgreifen, urteilt das Bundesverwaltungsgericht in Leipzig.

Lesezeit: 2 Min. In Pocket speichern 372

Suchen...

NETZPOLITIK.ORG

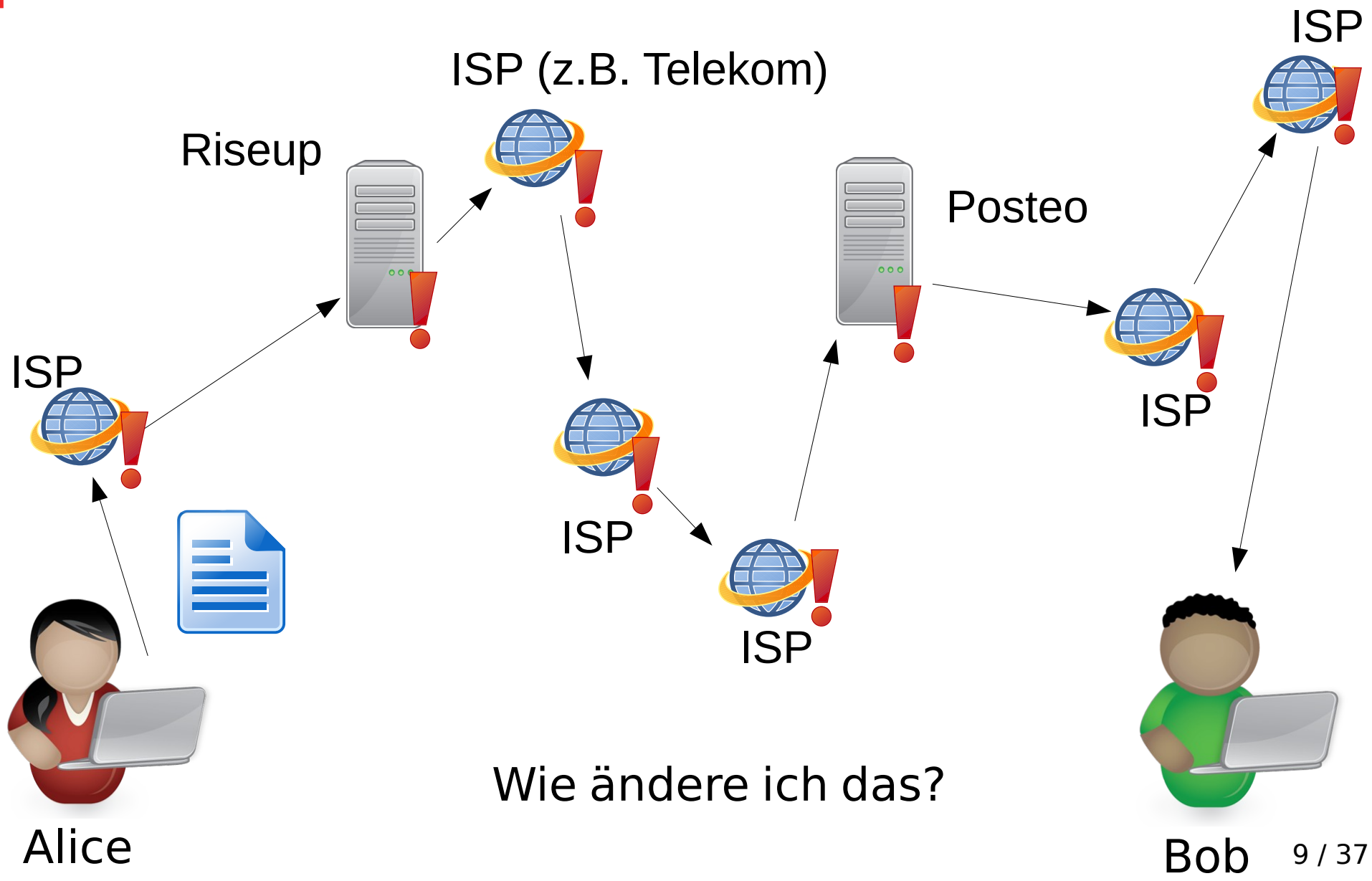
Bundesverfassungsgericht

Massenüberwachung im BND-Gesetz ist verfassungswidrig

Das BND-Gesetz verstößt gegen Grundrechte und ist grundrechtswidrig. Das hat das Bundesverfassungsgericht entschieden. Pressefreiheit und Telekommunikationsgeheimnis gelten nicht nur in Deutschland, deutsche Behörden müssen sich überall daran halten. Das Gesetz muss überarbeitet werden.

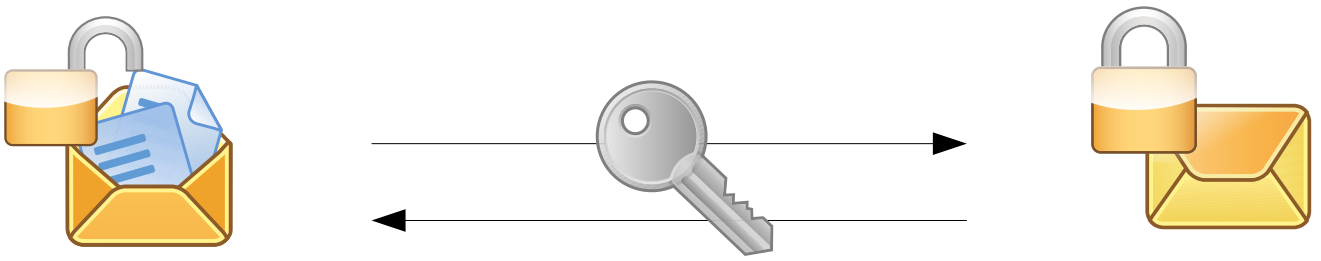
19.05.2020 um 10:30 Uhr - Andre Meister - in Überwachung - 15 Ergänzungen

Kommunikation im Internet



Wie ändere ich das?

Verschlüsselung!



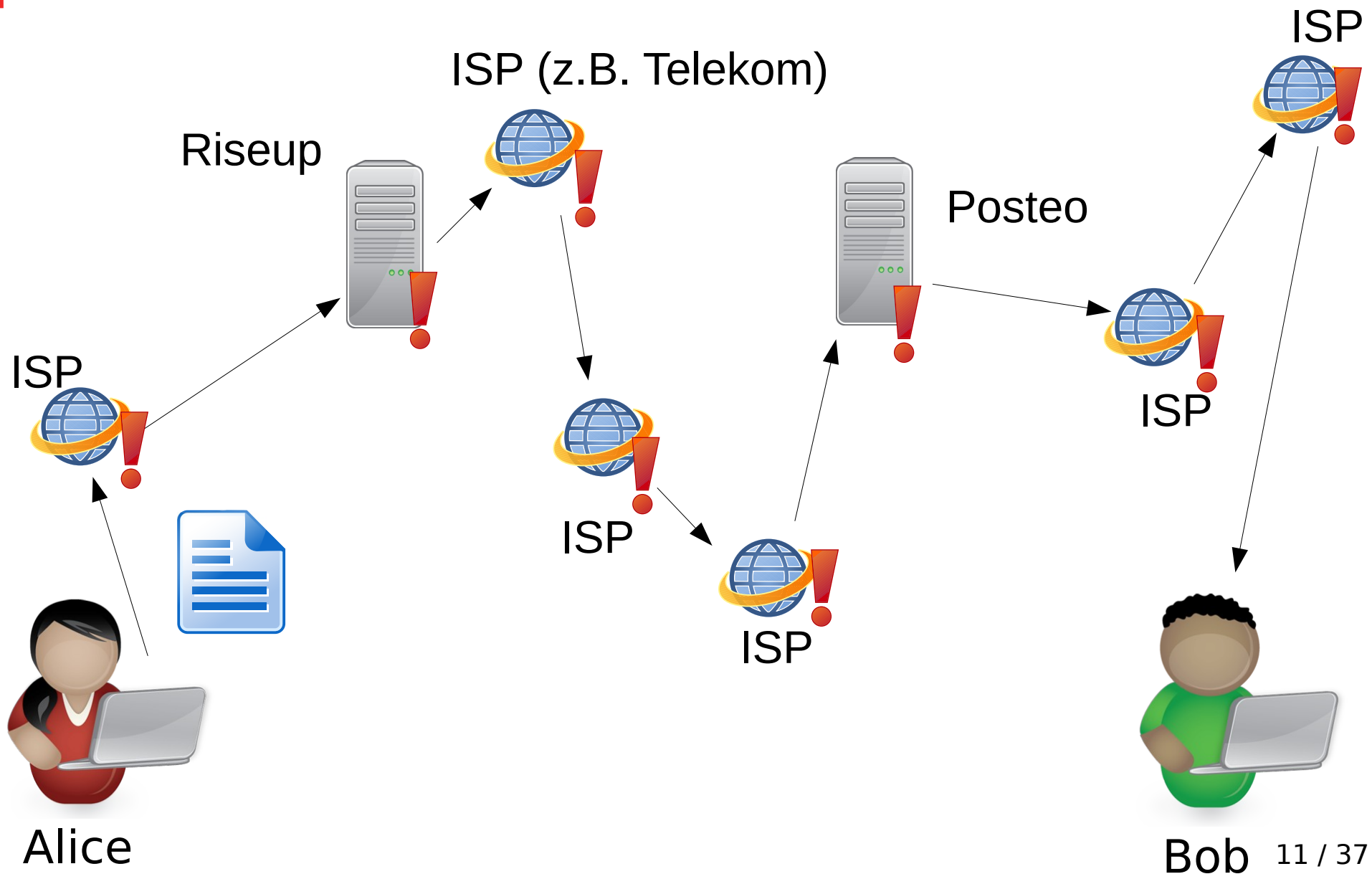
0x90

hallo :)

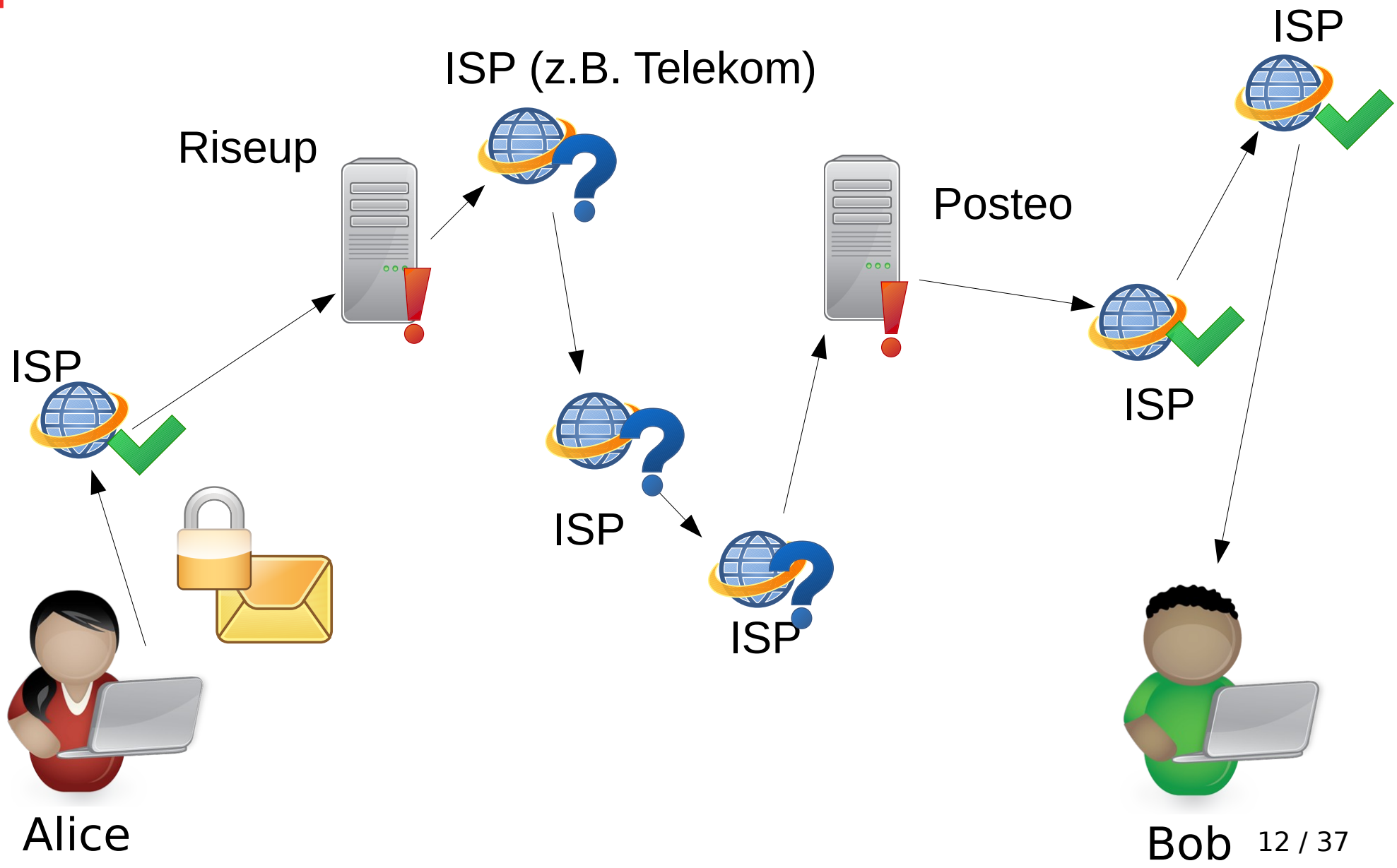
-----BEGIN PGP MESSAGE-----

jA0EBwMCWRjj8hKyyyfq0j4BHQH
C6vlddga/
+zu9XAhChkqOdOCiOIlY8h8hdekp
QP9p9iJ55MBglvPa0Xp5YACU3tM
4EgZtD+C5EI6YRQ==
=MQgn
-----END PGP MESSAGE-----

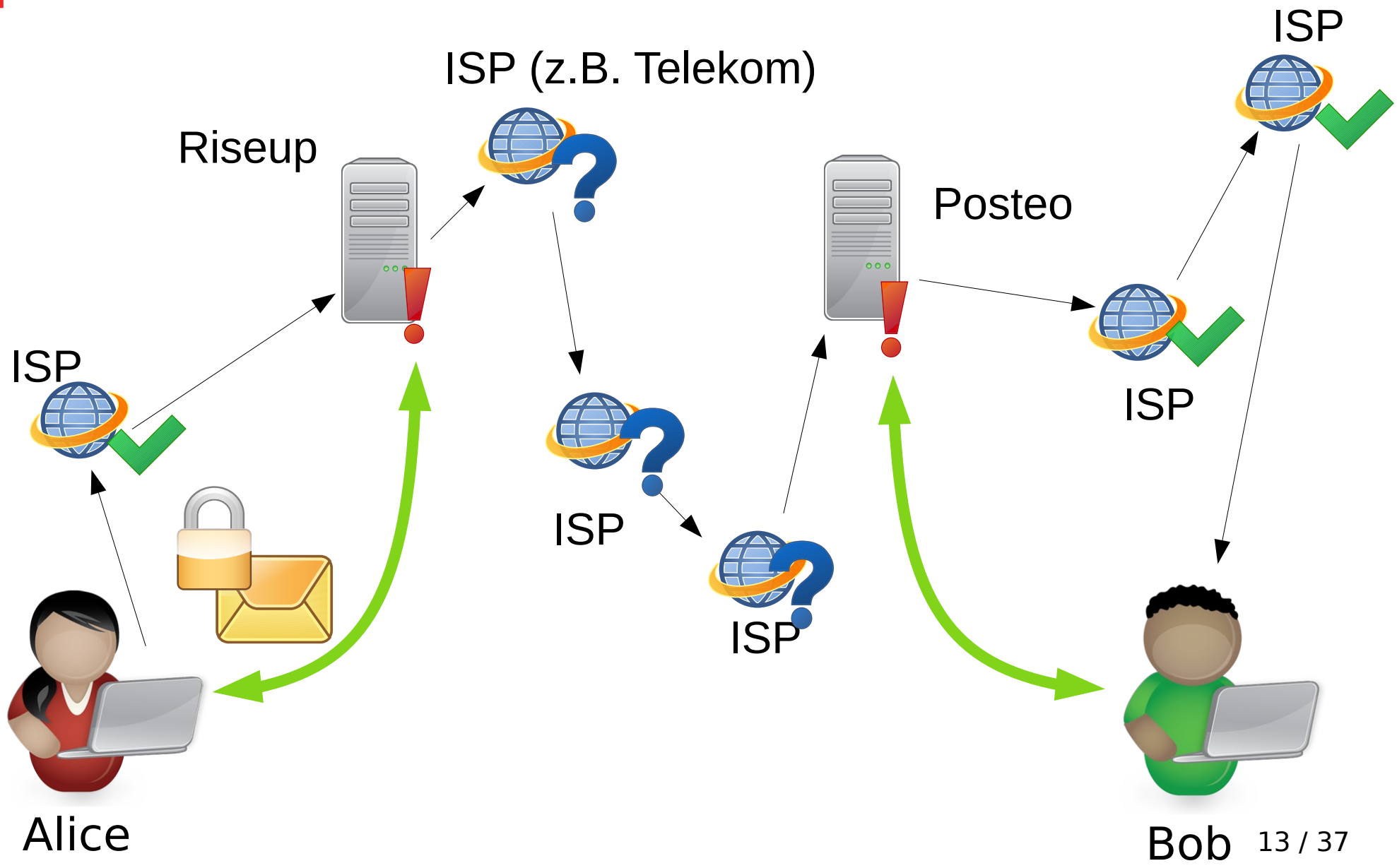
Kommunikation im Internet



Transportverschlüsselung

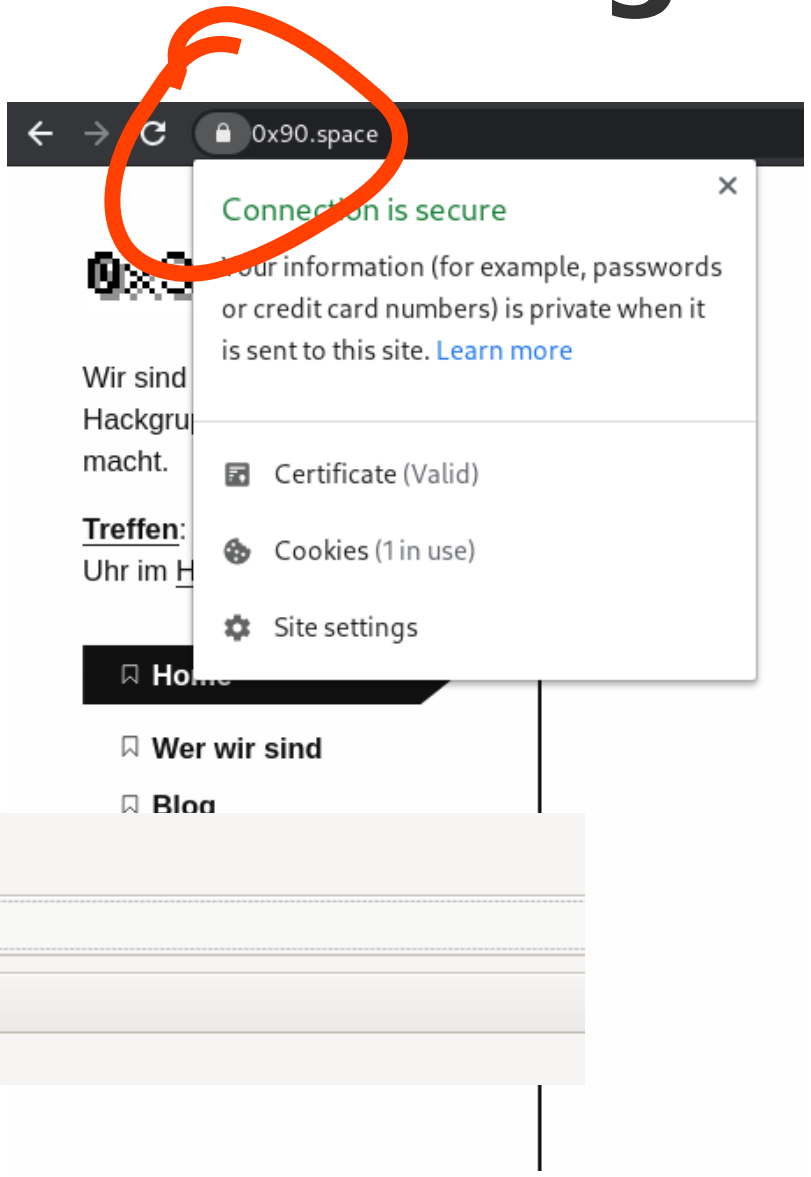


Transportverschlüsselung

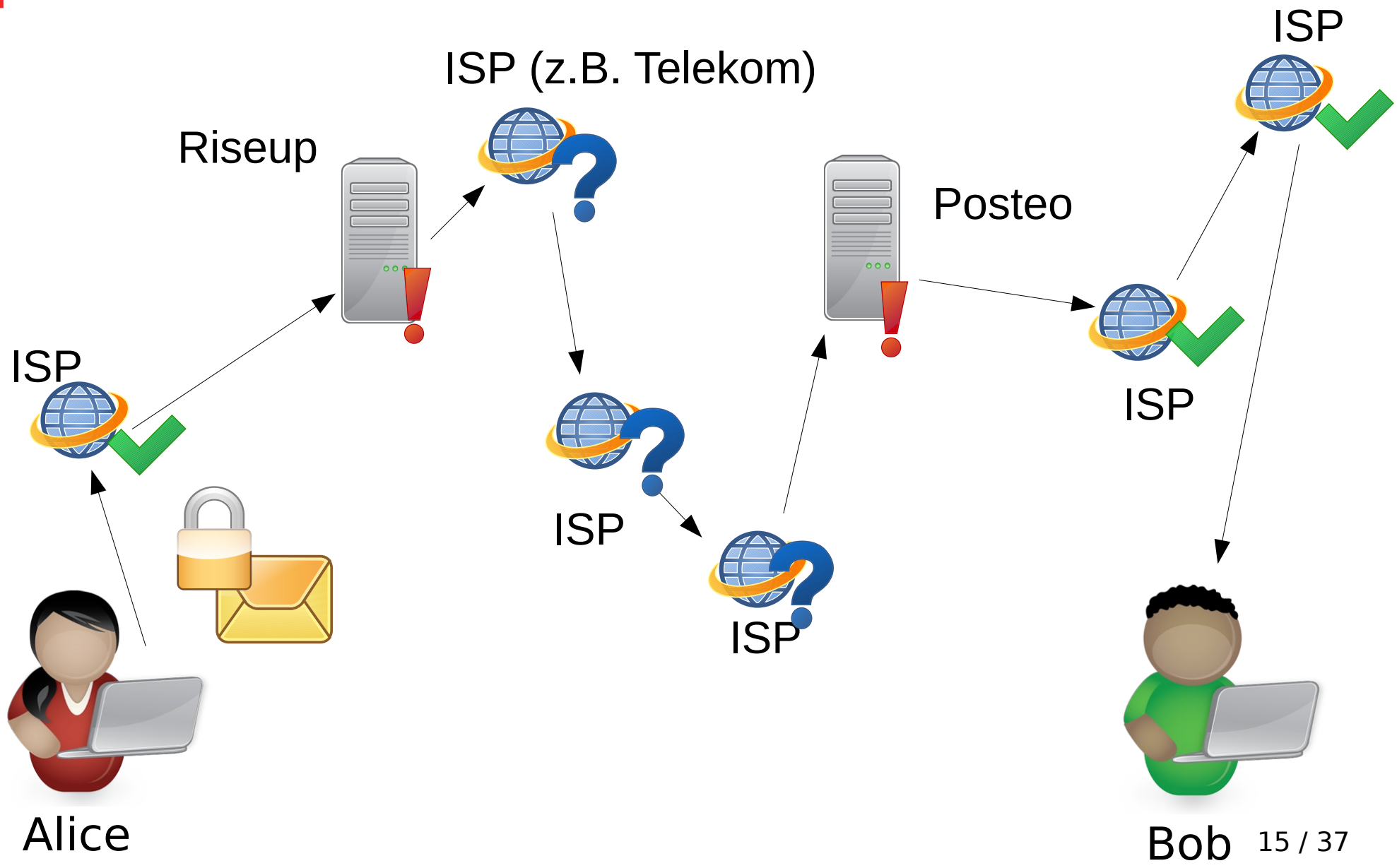


Transportverschlüsselung

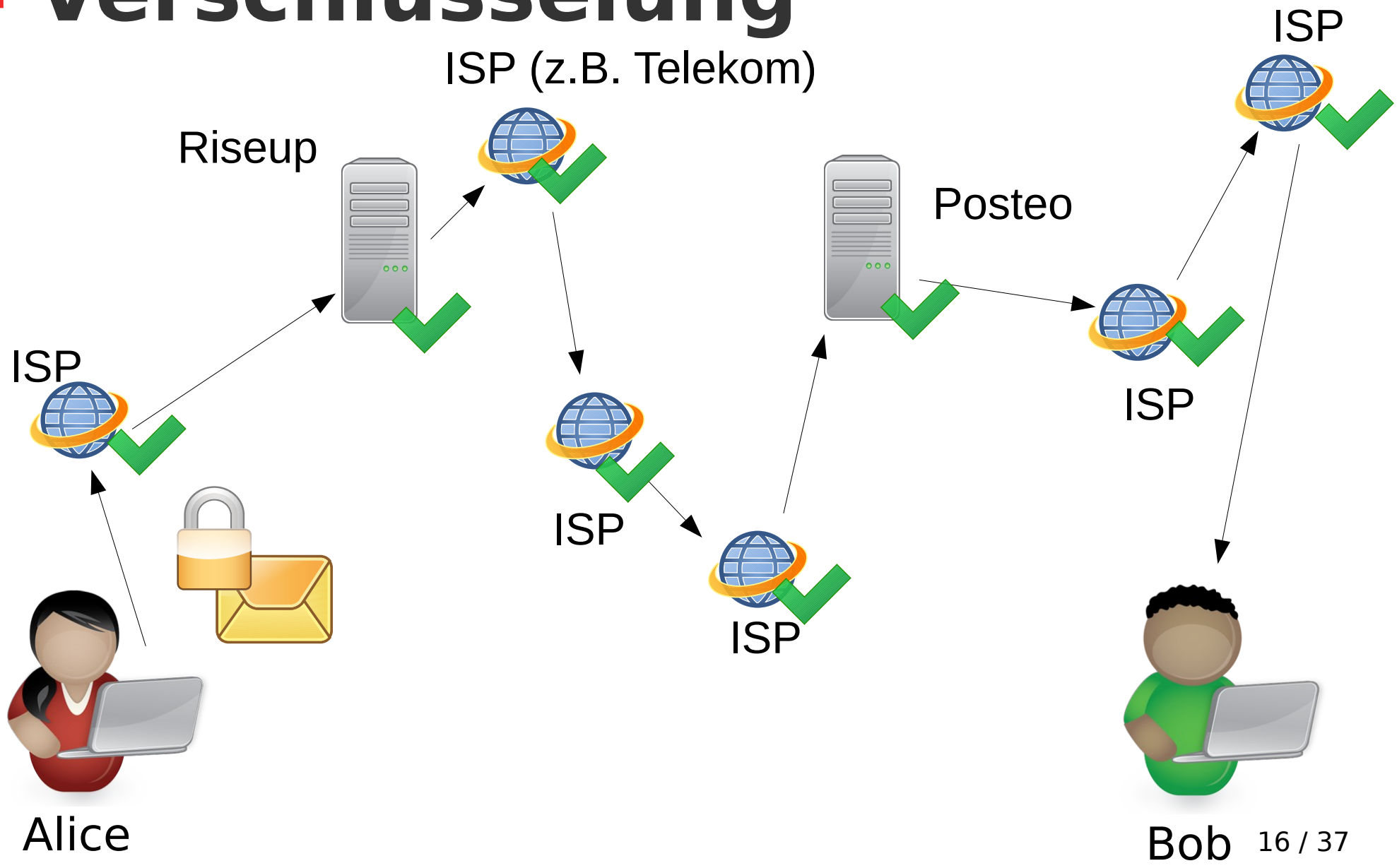
- Transportverschlüsselung ist weit verbreitet
  - SSL/TLS
  - STARTTLS



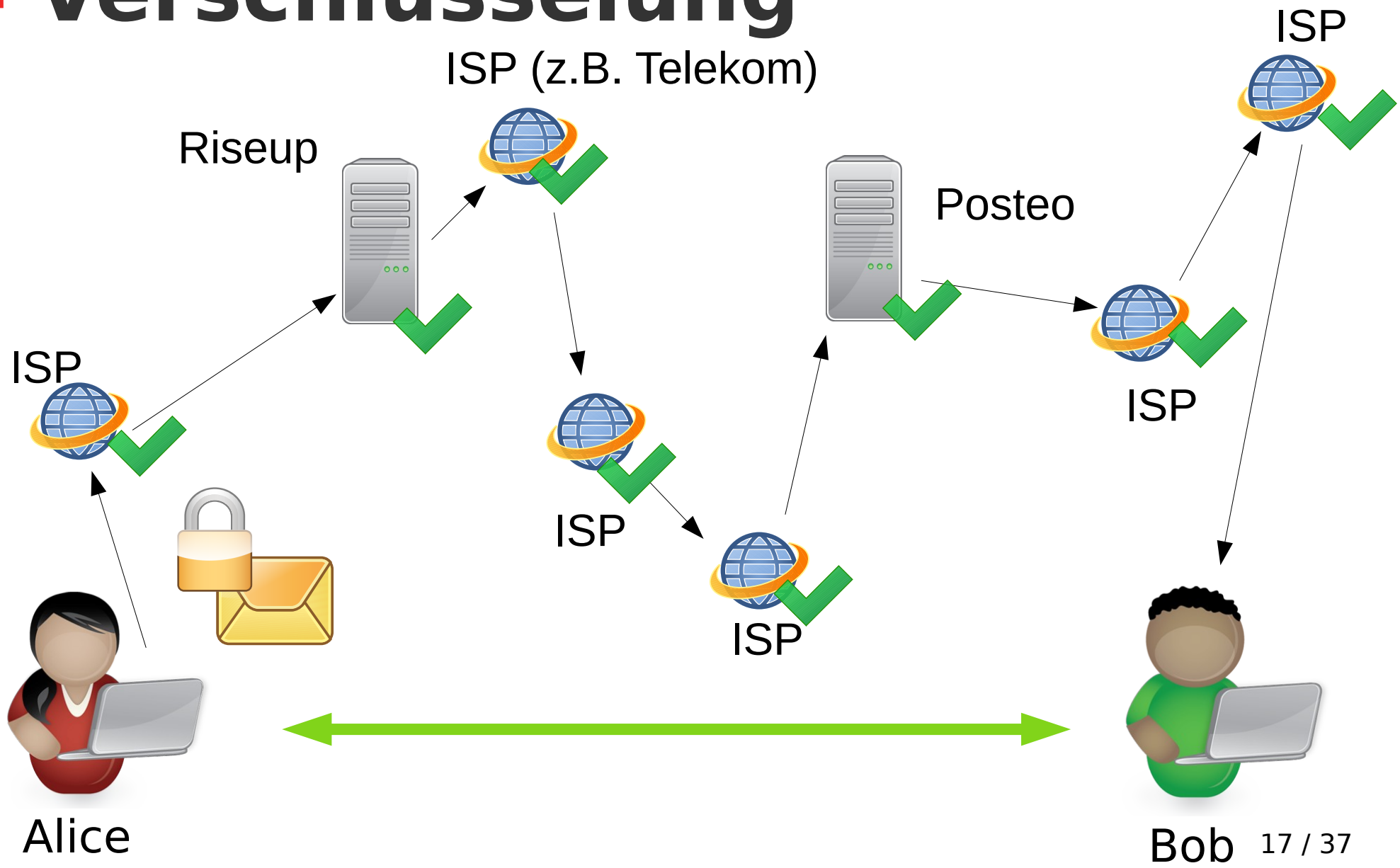
Transportverschlüsselung



Ende-zu-Ende-Verschlüsselung



Ende-zu-Ende-Verschlüsselung

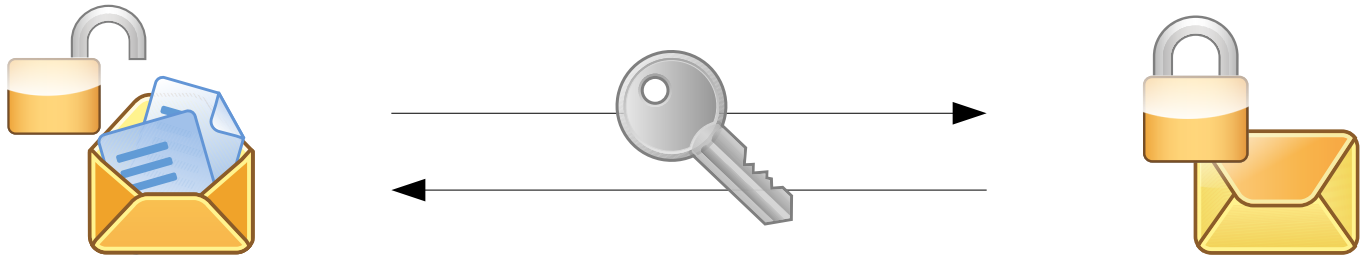


Ende-zu-Ende-Verschlüsselung

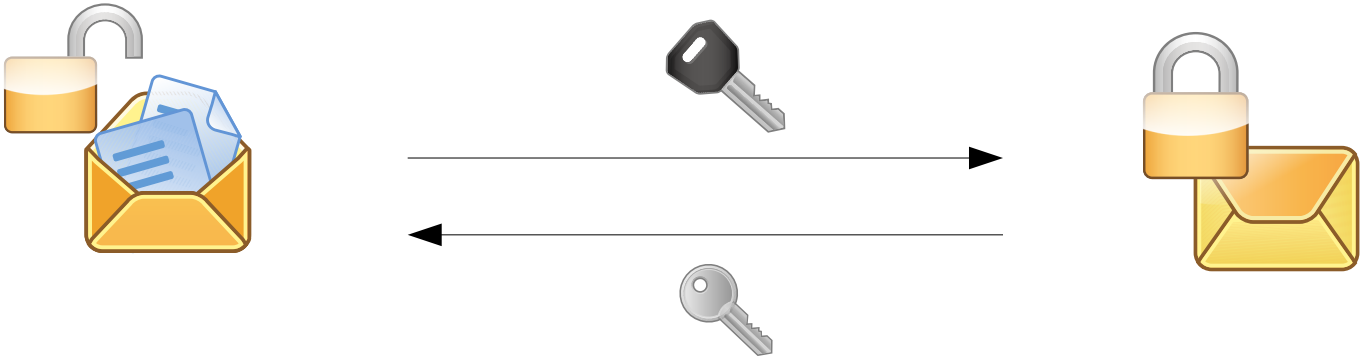
- Beispiele:
  - E-Mail mit PGP
  - Signal
  - Wire
  - Jabber mit OMEMO
  - ...

Verschlüsselung!

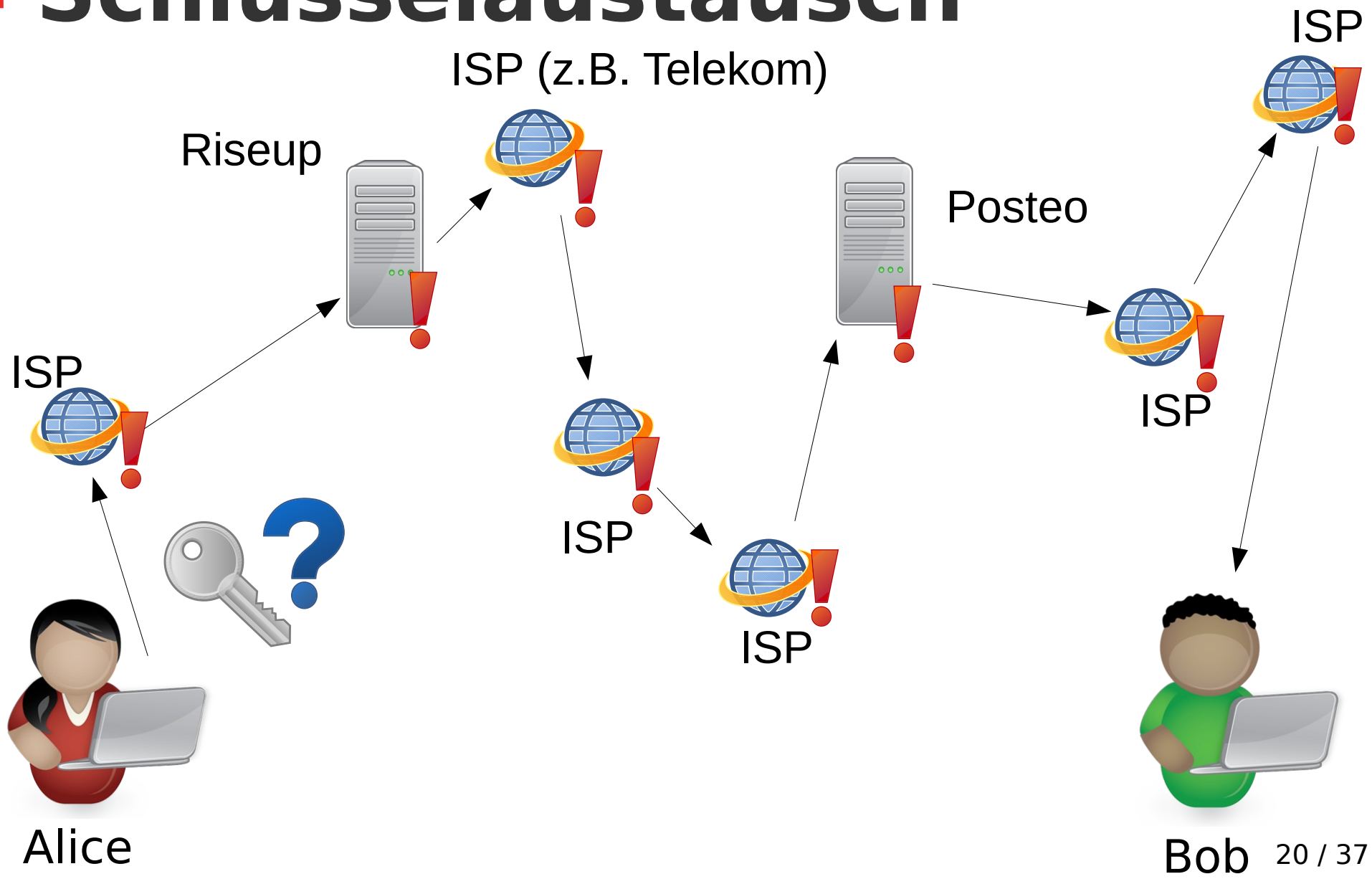
- Grundprinzipien:
  - **Symmetrische Verschlüsselung**



  - **Asymmetrische Verschlüsselung**

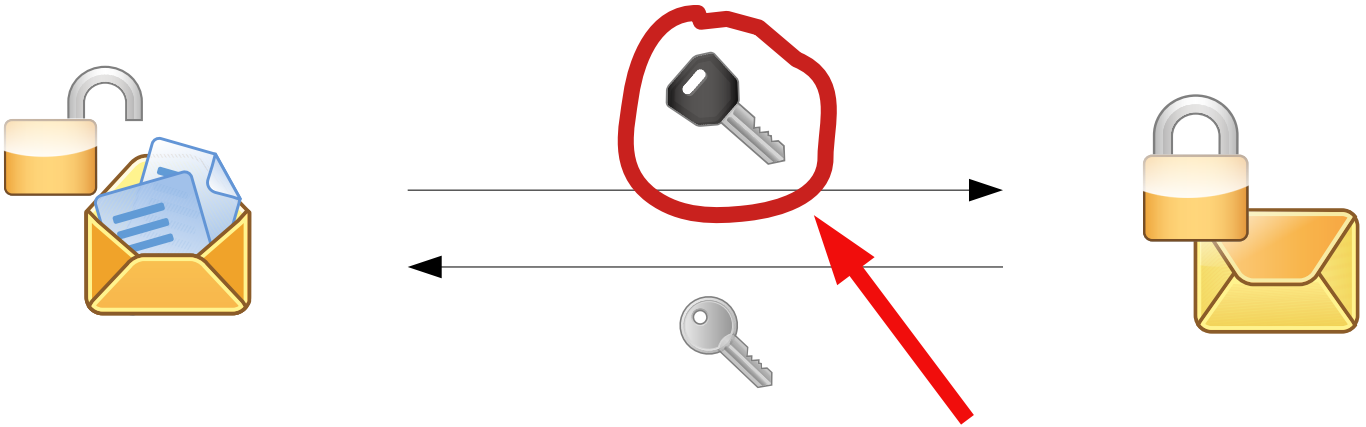


Problem: Schlüsselaustausch



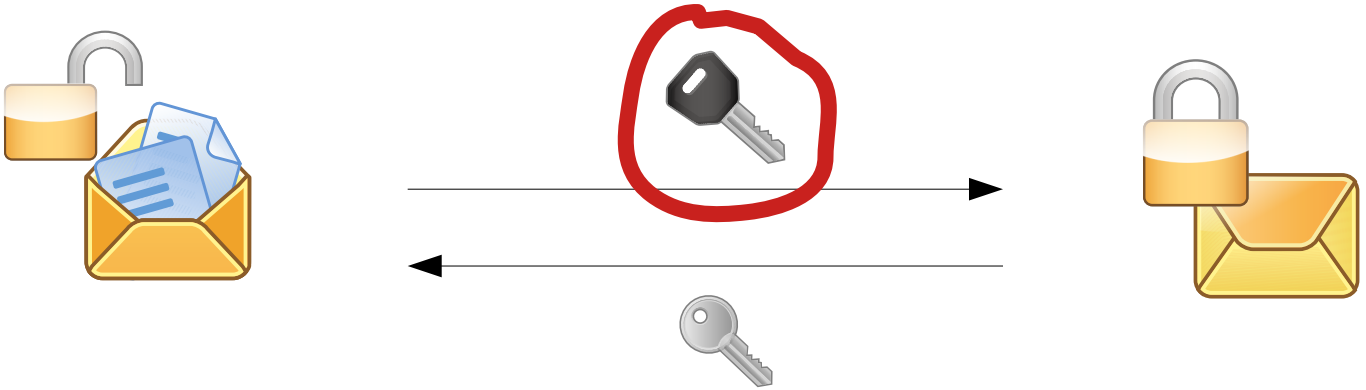
Problem: Schlüsselaustausch

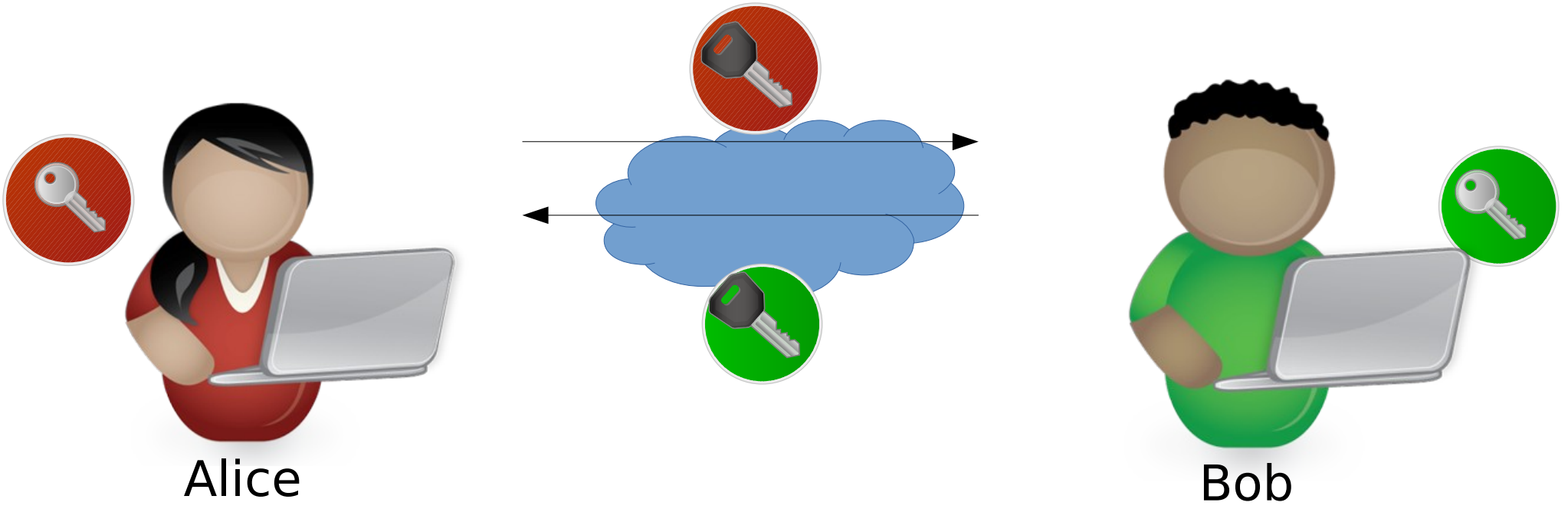
- Wie übergebe ich jemanden den Schlüssel im Internet???
  - **Symmetrische Verschlüsselung →** kompliziert
  - **Asymmetrische Verschlüsselung**



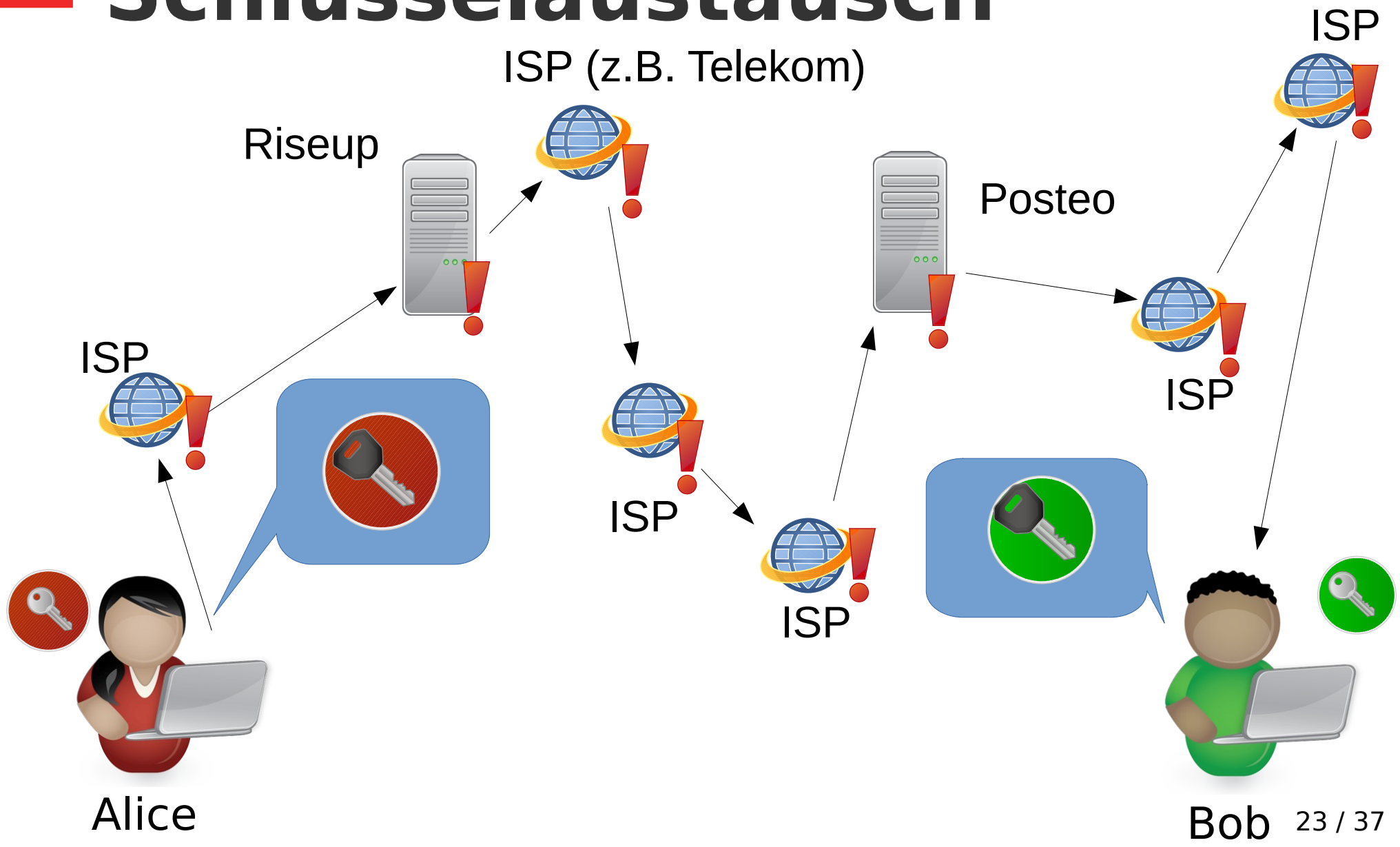
Ich kann diesen Schlüssel weitergeben!

Problem: Schlüsselaustausch

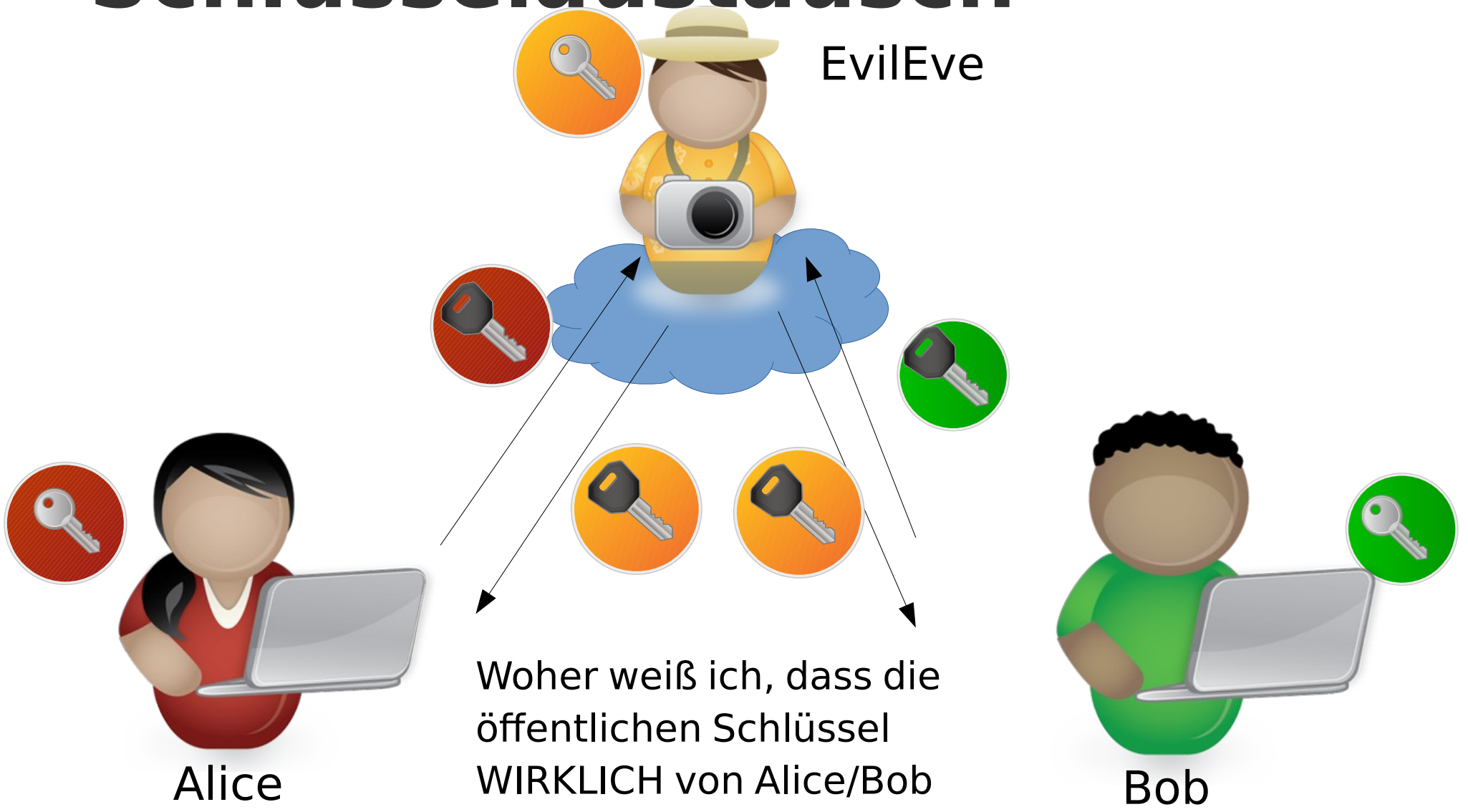




Problem: Schlüsselaustausch



Problem: Schlüsselaustausch



Woher weiß ich, dass die öffentlichen Schlüssel WIRKLICH von Alice/Bob kommen und nicht von Eve?

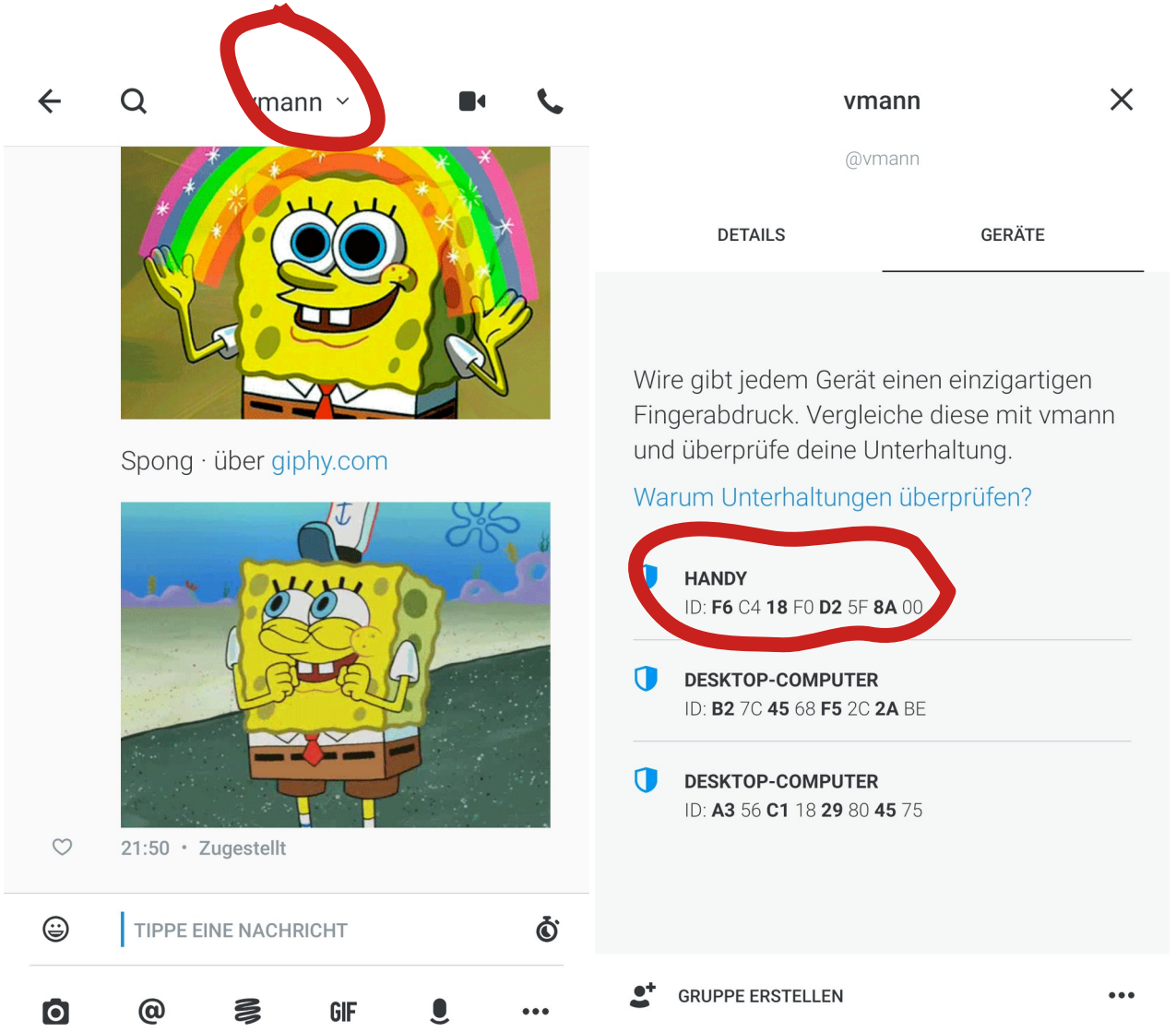
Ende-zu-Ende-Verschlüsselung

- Ende-zu-Ende-Verschlüsselung ist gut, wenn richtig angewendet
- Schützt vor passiven Angriffen (also passiv alles Mitschneiden wie z.B. strategische TKÜ geht nicht)
- Bei einem aktiven Angriff (z.B. durch EvilEve) ist es bei korrekter Anwendungsweise sicher
  → wie wendet man es korrekt an?

Fingerprints vergleichen

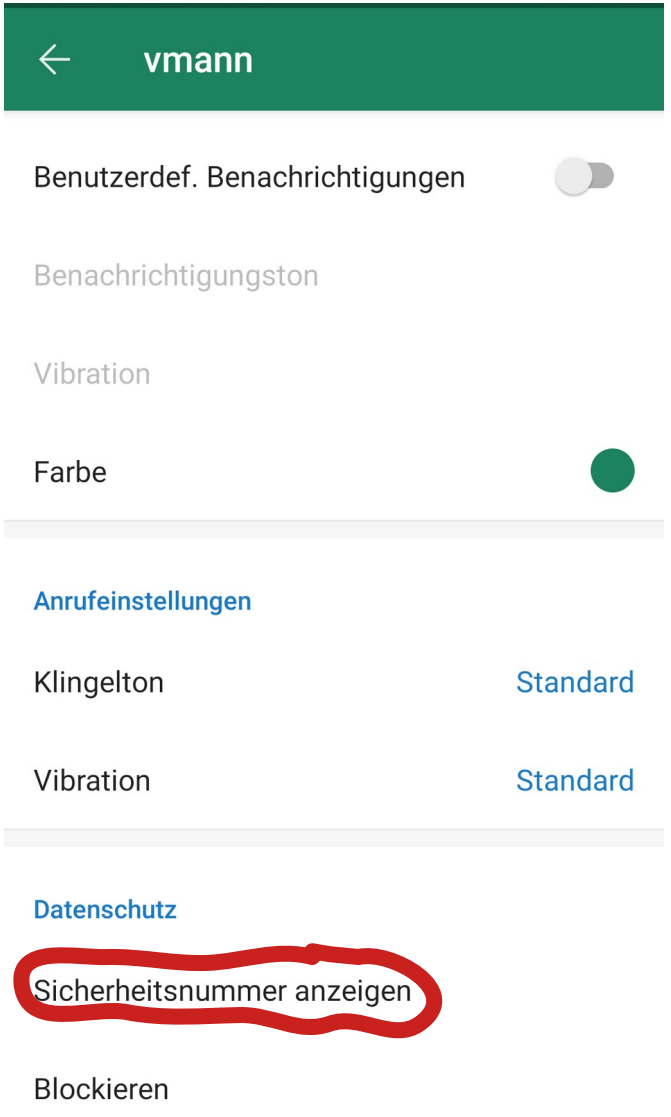
- Fingerprints sind Zahlen, die einen öffentlichen Schüssel identifizieren
  - Prüft den Fingerprint gegenseitig um sicherzustellen, dass ihr die echten Schlüssel habt! (z.B. Treffen, Telefonieren+Vorlesen, etc)
  - Immer dann notwendig, wenn sich der öffentliche Schlüssel ändert (z.B. neues Gerät)

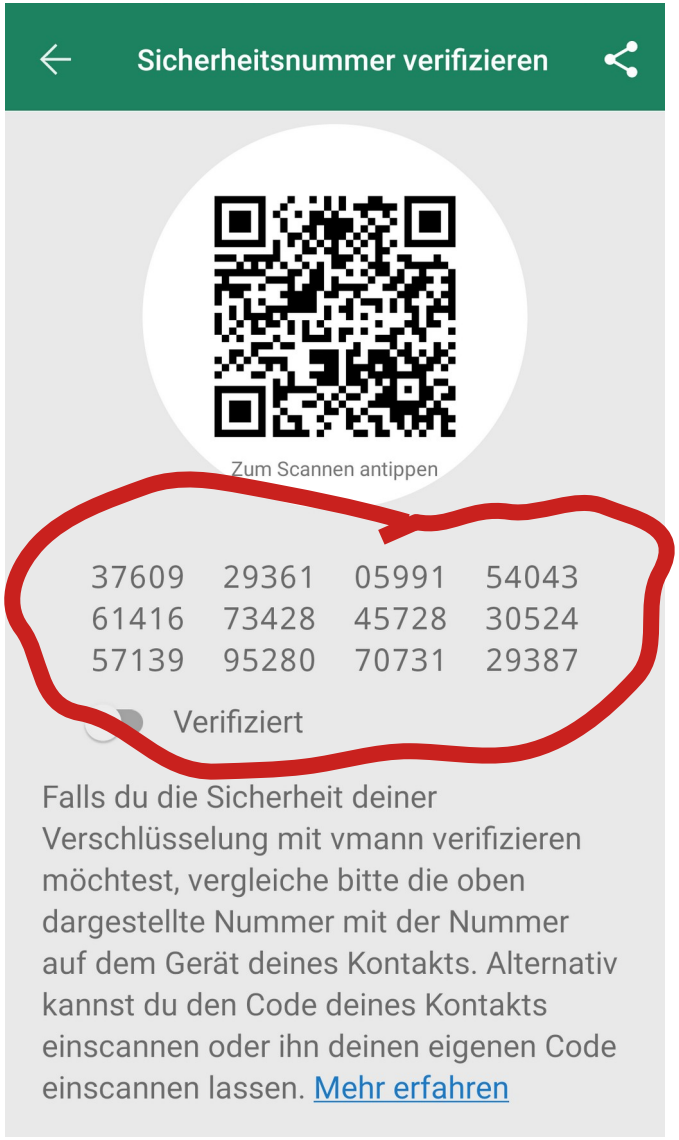
Beispiel: Wire



Beispiel: Wire Teil 2

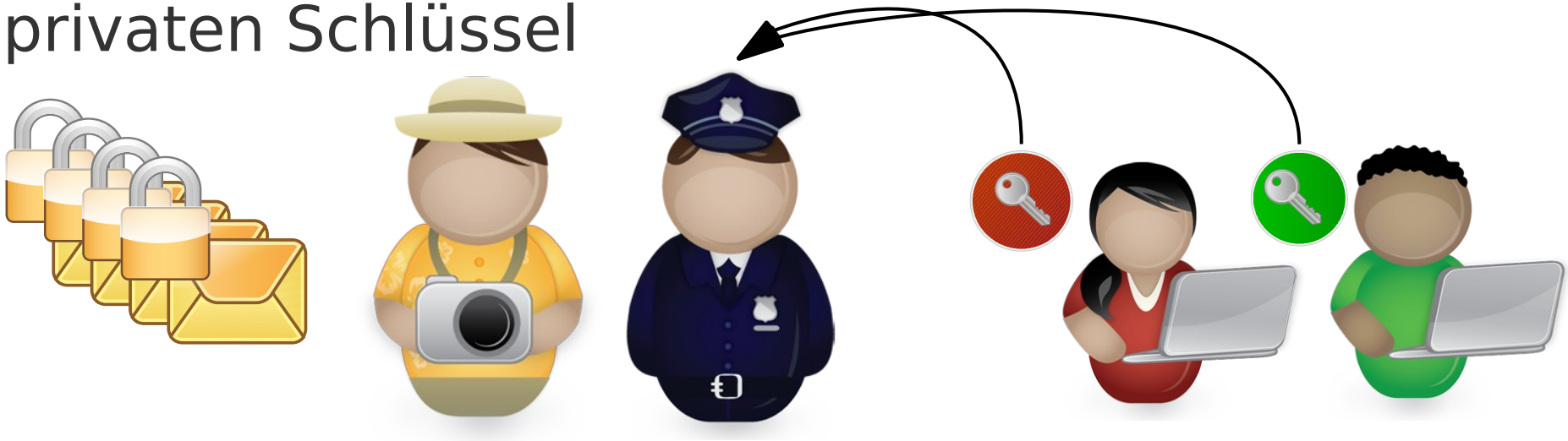
Beispiel: Signal





Forward Secrecy

- Problem: Überwacher sammelt verschlüsselte Nachrichten und kommt später an die privaten Schlüssel

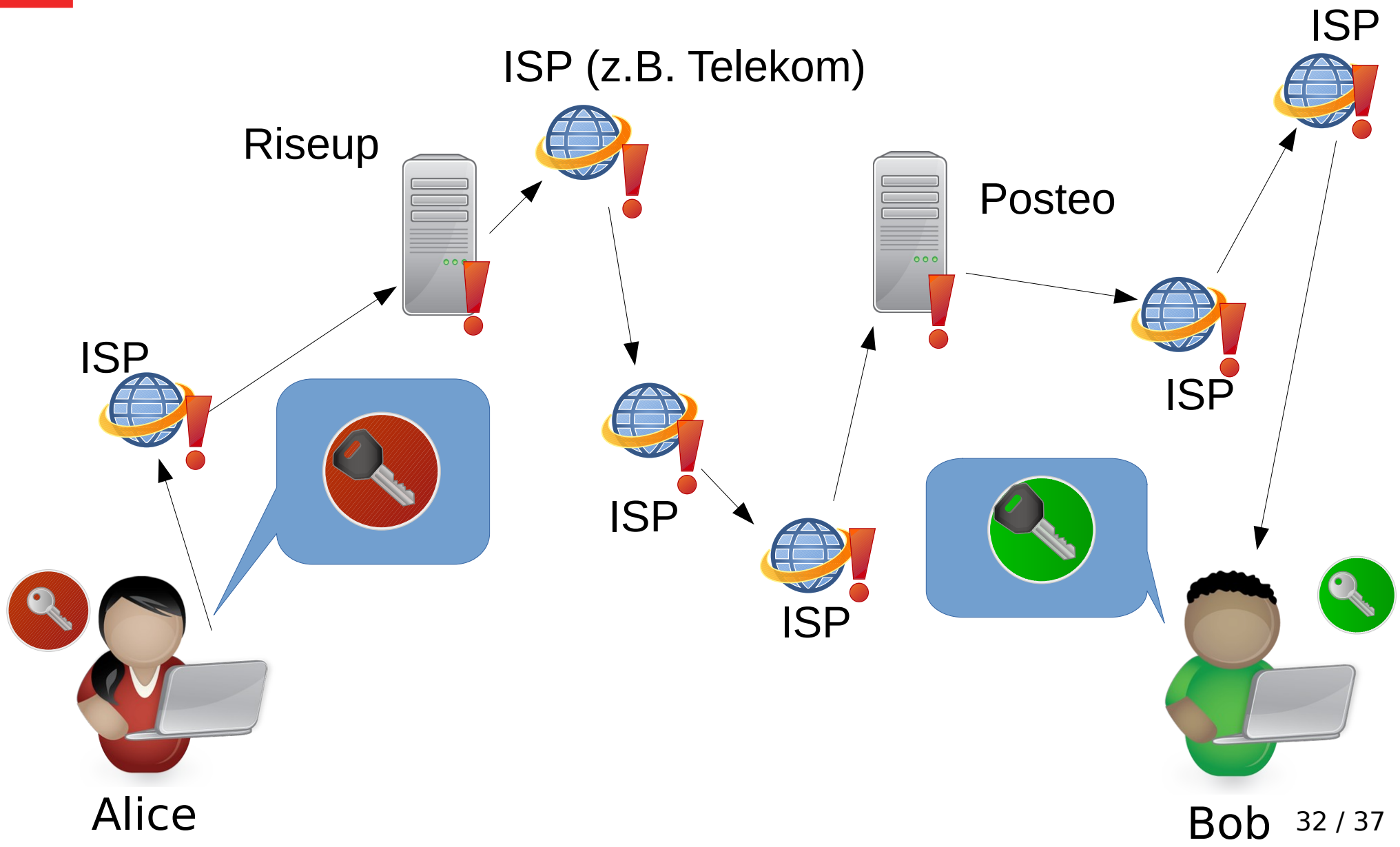


- Lösung: neue Schlüssel pro Nachricht
- Implementiert in Signal/Wire/OMEMO, aber **nicht** in PGP

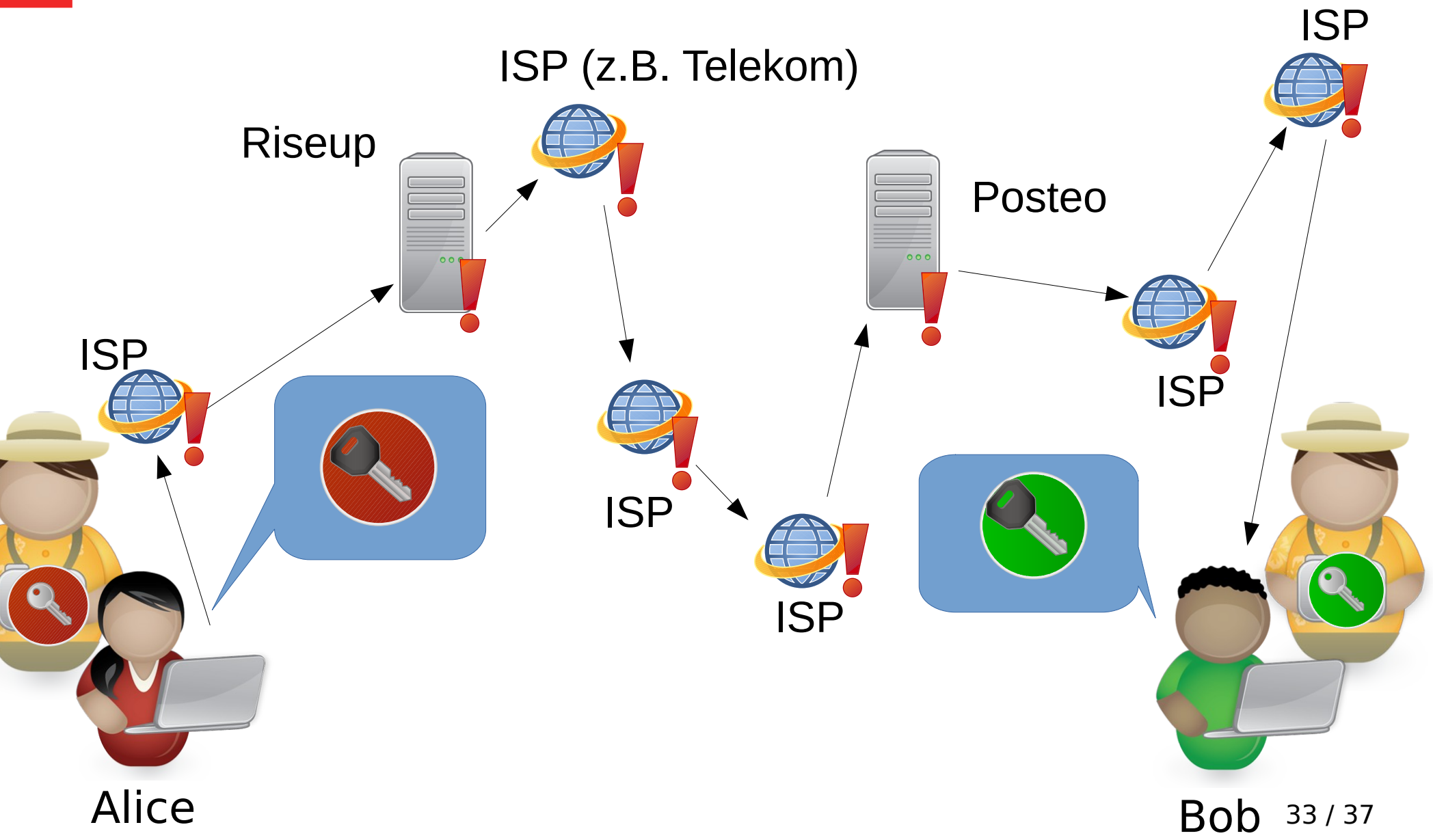
Grenzen der Ende-zu-Ende-Verschlüsselung

- Ende-zu-Ende-Verschlüsselung stellt sogar staatliche Angreifer auf die Probe
- Reaktion:
  - Quellen TKÜ (§100a StPO) → Trojaner
  - Online-Durchsuchung (§100b StPO) → Trojaner
  - Forderungen nach Backdoors in Verschlüsselungsimplementierungen

Trojaner und Backdoors



Trojaner und Backdoors



Grenzen der Ende-zu-Ende-Verschlüsselung

- Staatstrojaner vermindern die Sicherheit **aller** Nutzer!
  - Sicherheitslücken werden verkauft, statt behoben
  - Interessenverschiebung: staatliches Interesse daran, dass Software unsicher ist
    - (berechtigtes) Misstrauen gegen staatliche Sicherheitsinitiativen
  - Unbehobene Lücken können von beliebigen Akteuren genutzt werden

Grenzen der Ende-zu-Ende-Verschlüsselung

- Ende-zu-Ende-Verschlüsselung verschleiert **nicht** wer mit wem kommuniziert
- Präventive Speicherung unter der sogen. “Vorratsdatenspeicherung”
  - 2008 in Kraft
  - 2010 verfassungswidrig erklärt (BVG)
  - 2015 neu in Kraft
  - 2016 illegal erklärt (EuGH)
  - 2017 “faktisch ausgesetzt”

Zusammenfassung

- Ende-zu-Ende-Verschlüsselung ist ein effektives Mittel den Inhalt von Nachrichten auf dem gesamten Weg vom Sender zum Empfänger geheim zu halten
- Durch das Prüfen der Fingerprints können aktive Angriffe aus dem Netz verhindert werden
- Grenzen der Ende-zu-Ende-Verschlüsselung sind unter anderem:
  - Fehlende Beseitigung von Metadaten
  - Kompromittierte Endgeräte

Fragen?