



# **Verschlüsselte Kommunikation**

Panda & vmann



# Inhalt

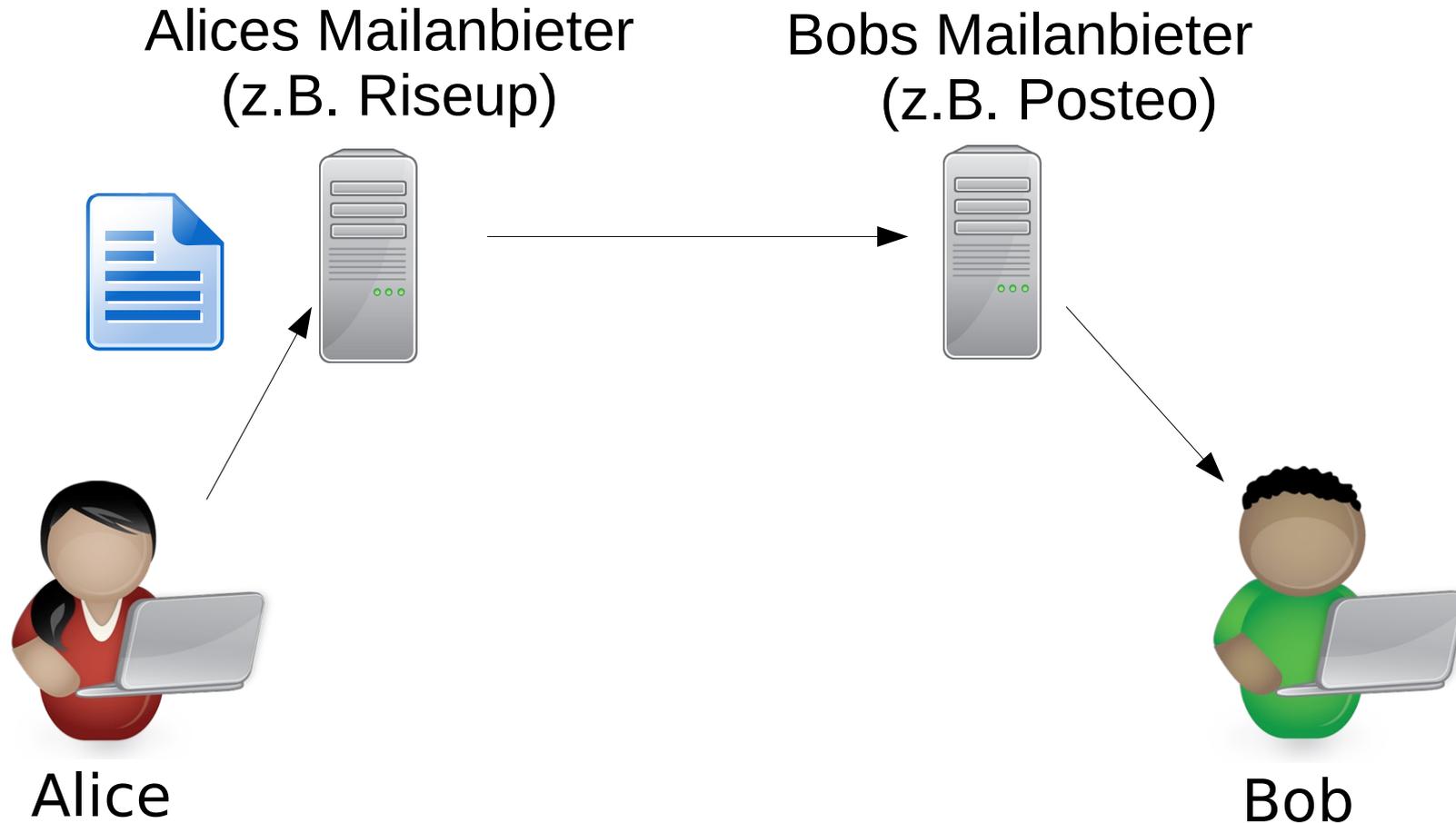
- Verschlüsselung in Netzwerken – warum?
- Verschlüsselung 101
- Ende-zu-Ende-Verschlüsselung
  - Sichere Nutzung
  - Forward Secrecy
  - Grenzen

# Kommunikation im Internet



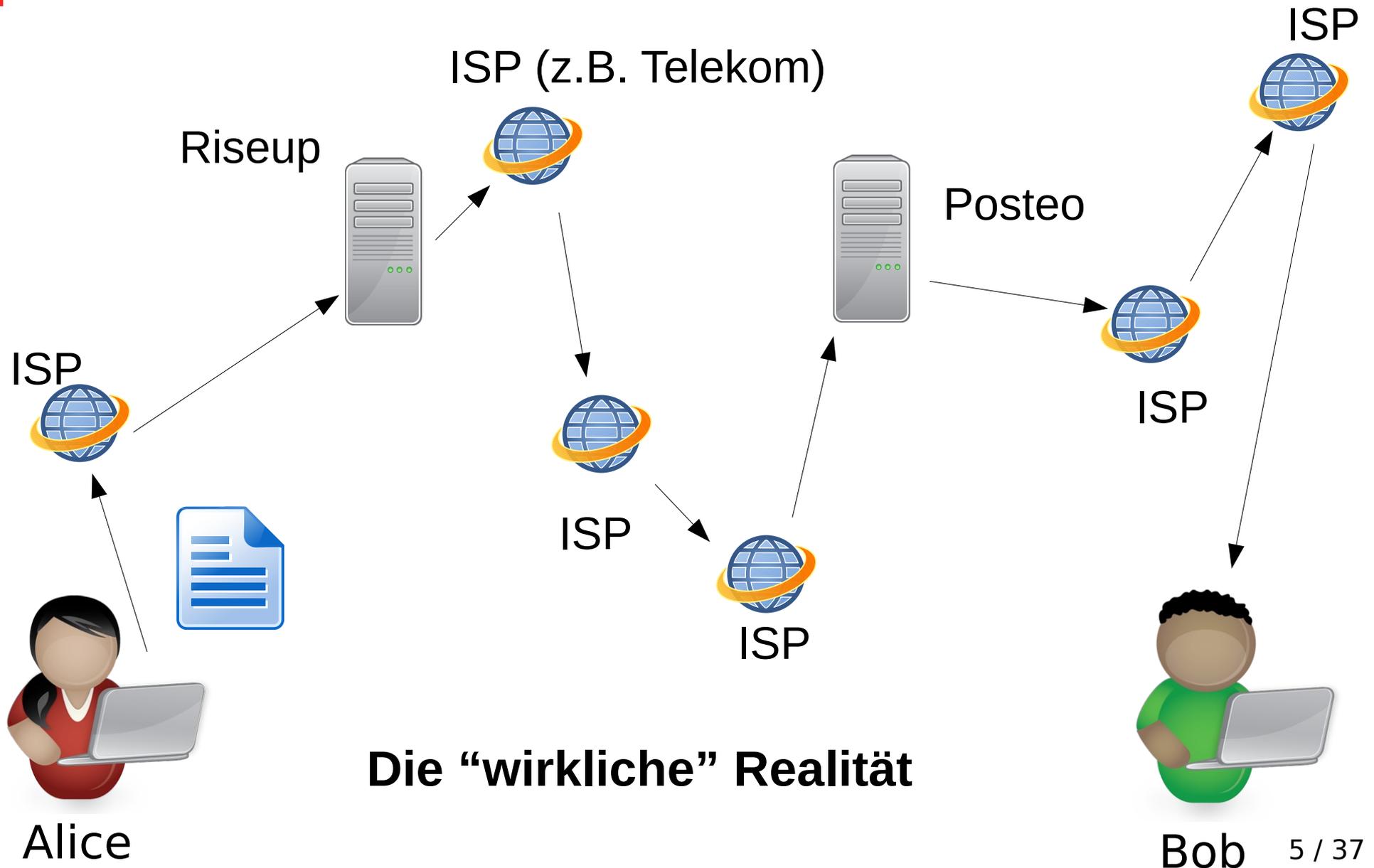
**Die Idee**

# Kommunikation im Internet

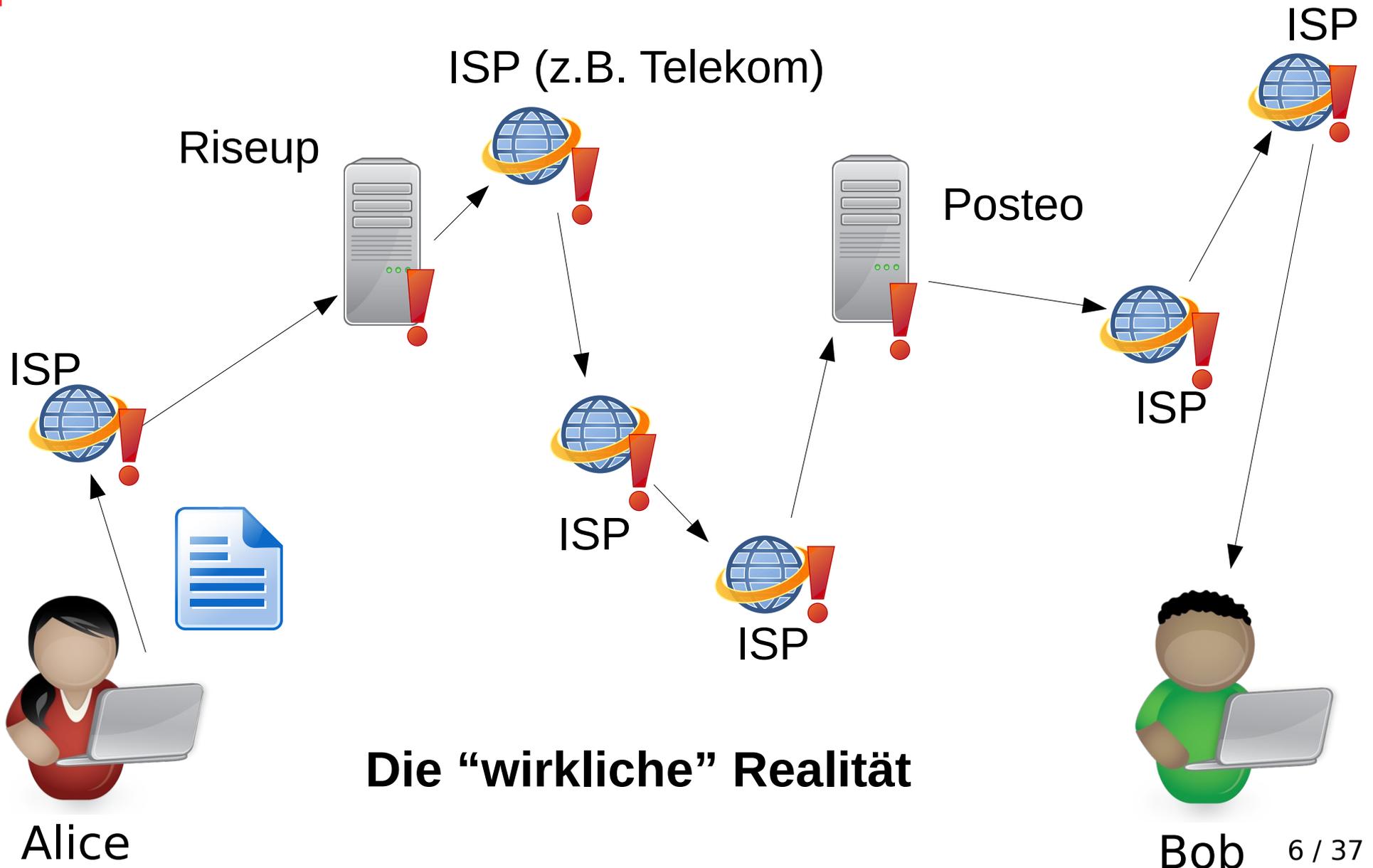


**Die Realität**

# Kommunikation im Internet



# Kommunikation im Internet



# “Lawful” Interception

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

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

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

Lesezeit: 2 Min.  In Pocket speichern

   372



## ISP



Suchen...  **NETZPOLITIK.ORG**

**Bundesverfassungsgericht**

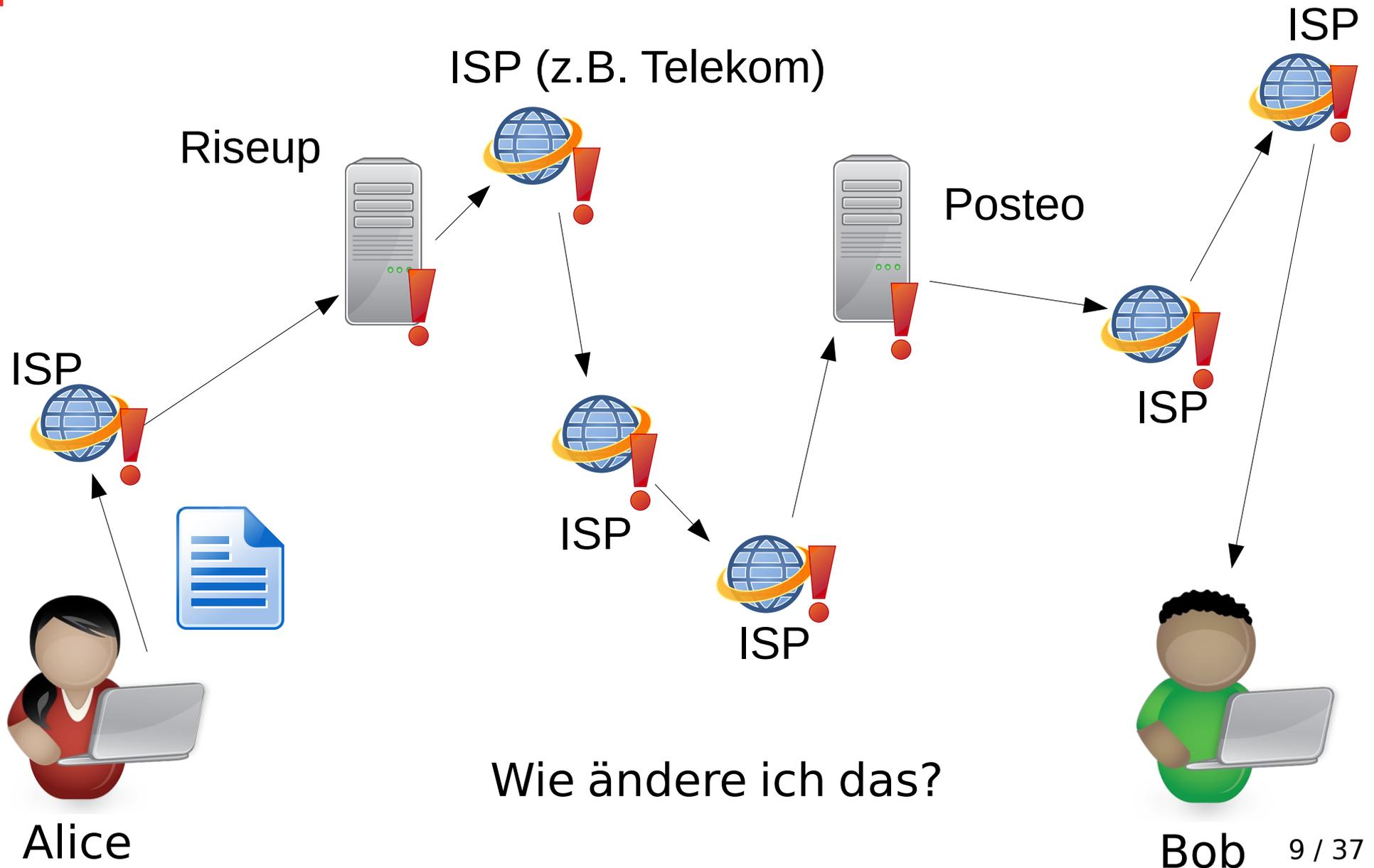
### Massenüberwachung im BND-Gesetz ist verfassungswidrig

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



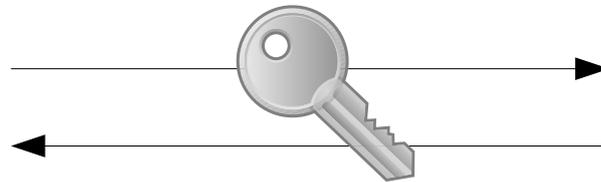
# Kommunikation im Internet



# Verschlüsselung!



hallo :)



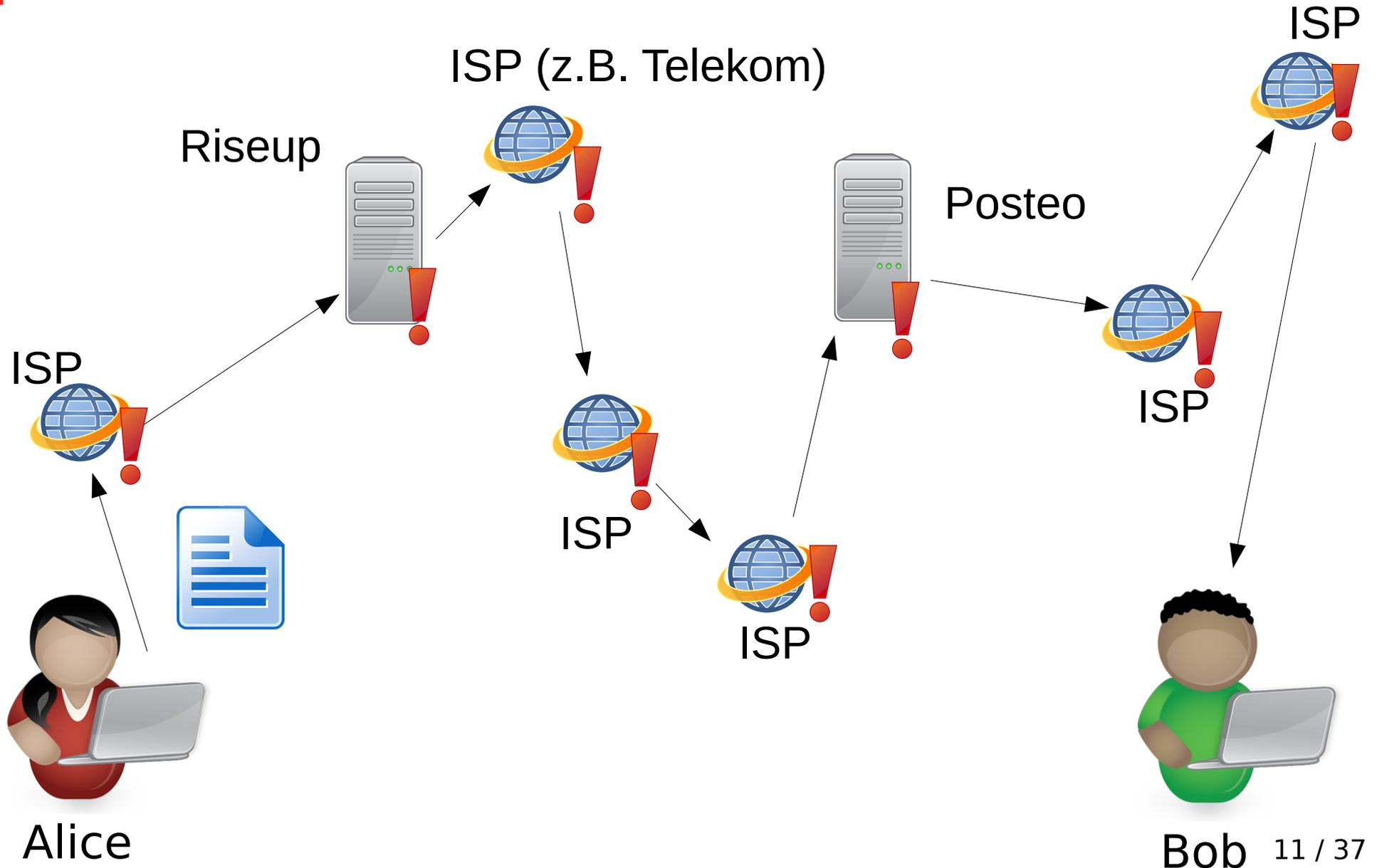
0x90



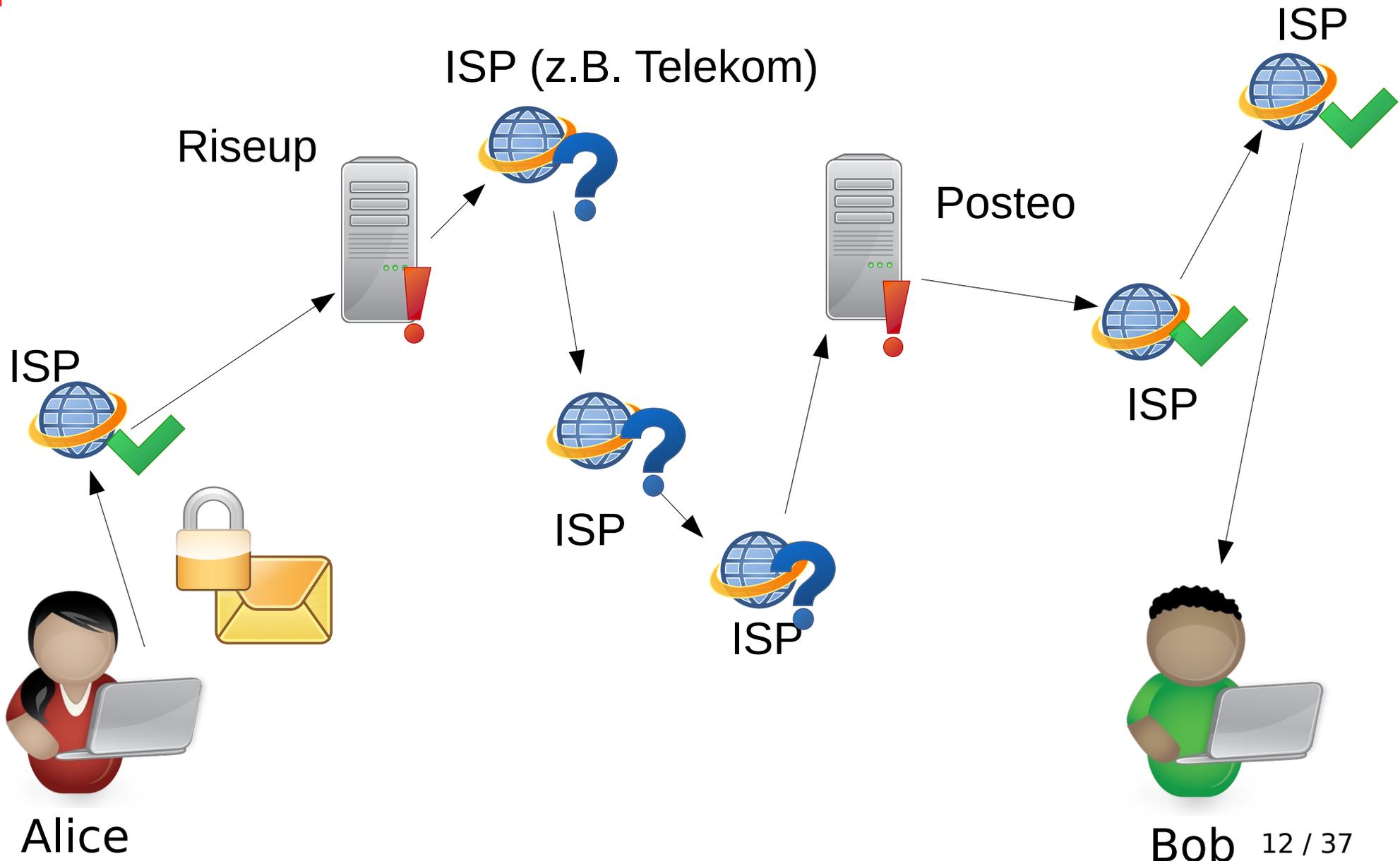
-----BEGIN PGP MESSAGE-----

```
jA0EBwMCWRjj8hKyyyyfq0j4BHQH  
C6vlddga/  
+zu9XAhChkqOdOCiOIIY8h8hdekp  
QP9p9iJ55MBglvPa0Xp5YACU3tM  
4EgZtD+C5EI6YRQ==  
=MQgn  
-----END PGP MESSAGE-----
```

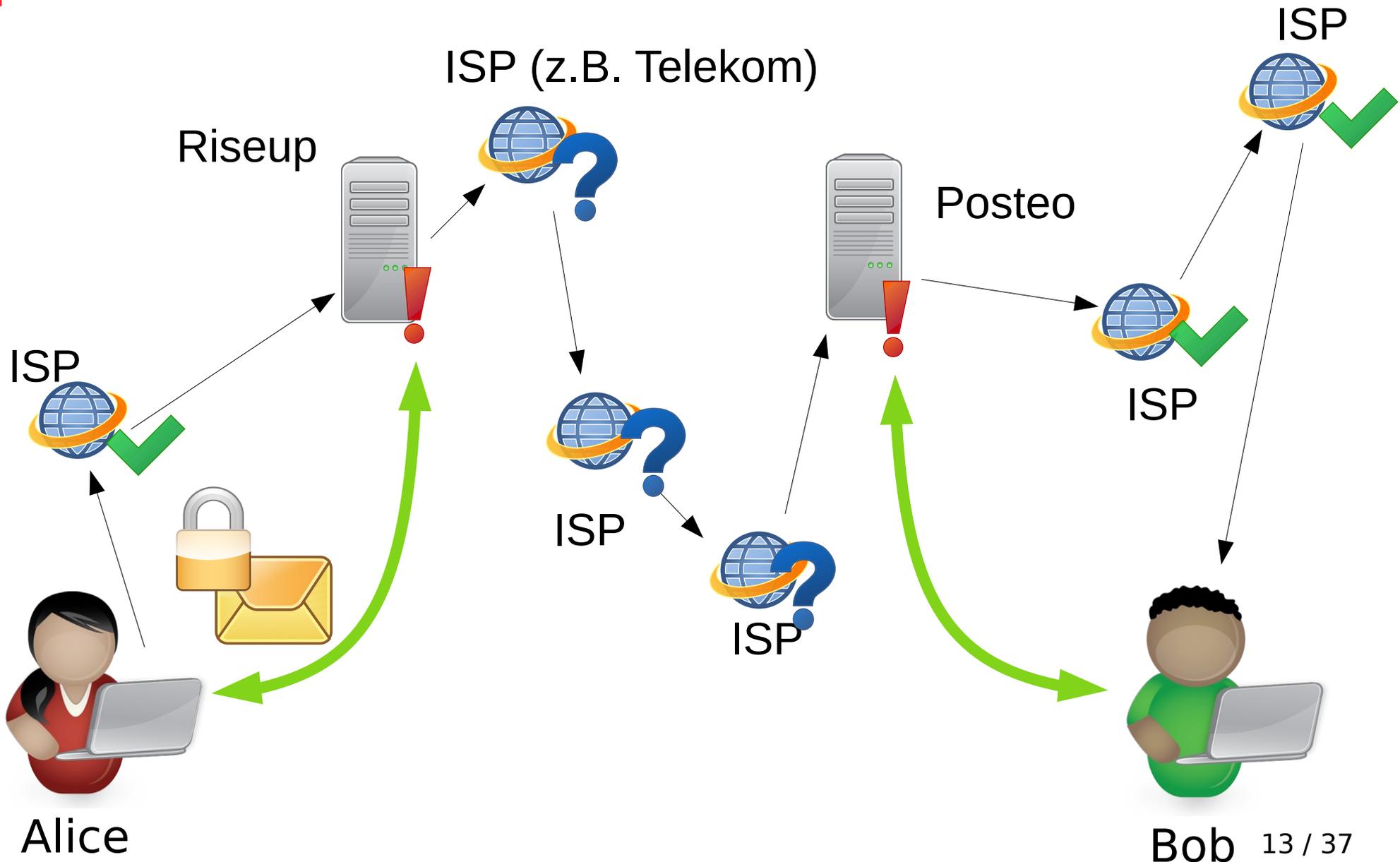
# Kommunikation im Internet



# Transportverschlüsselung

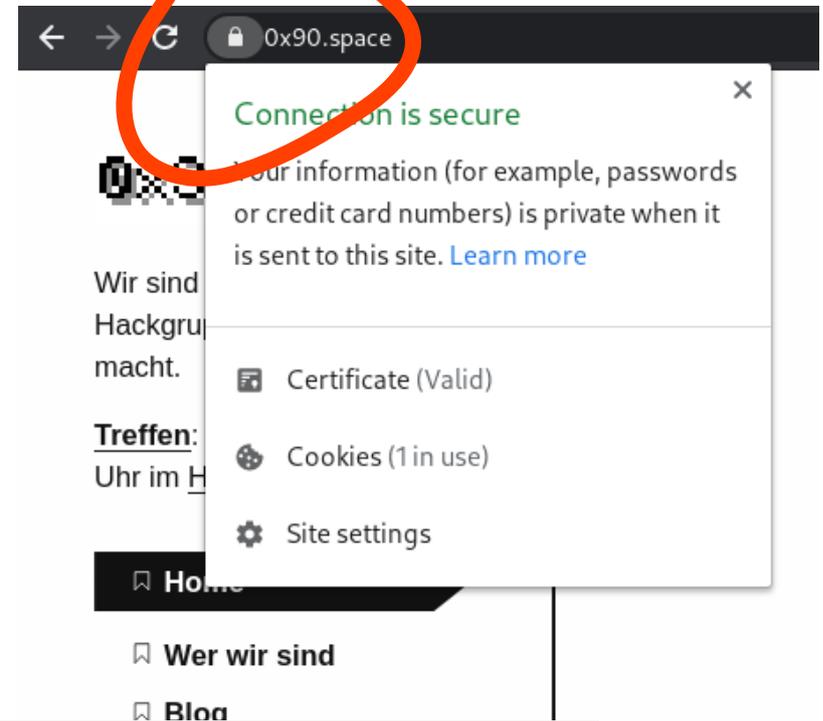


# Transportverschlüsselung

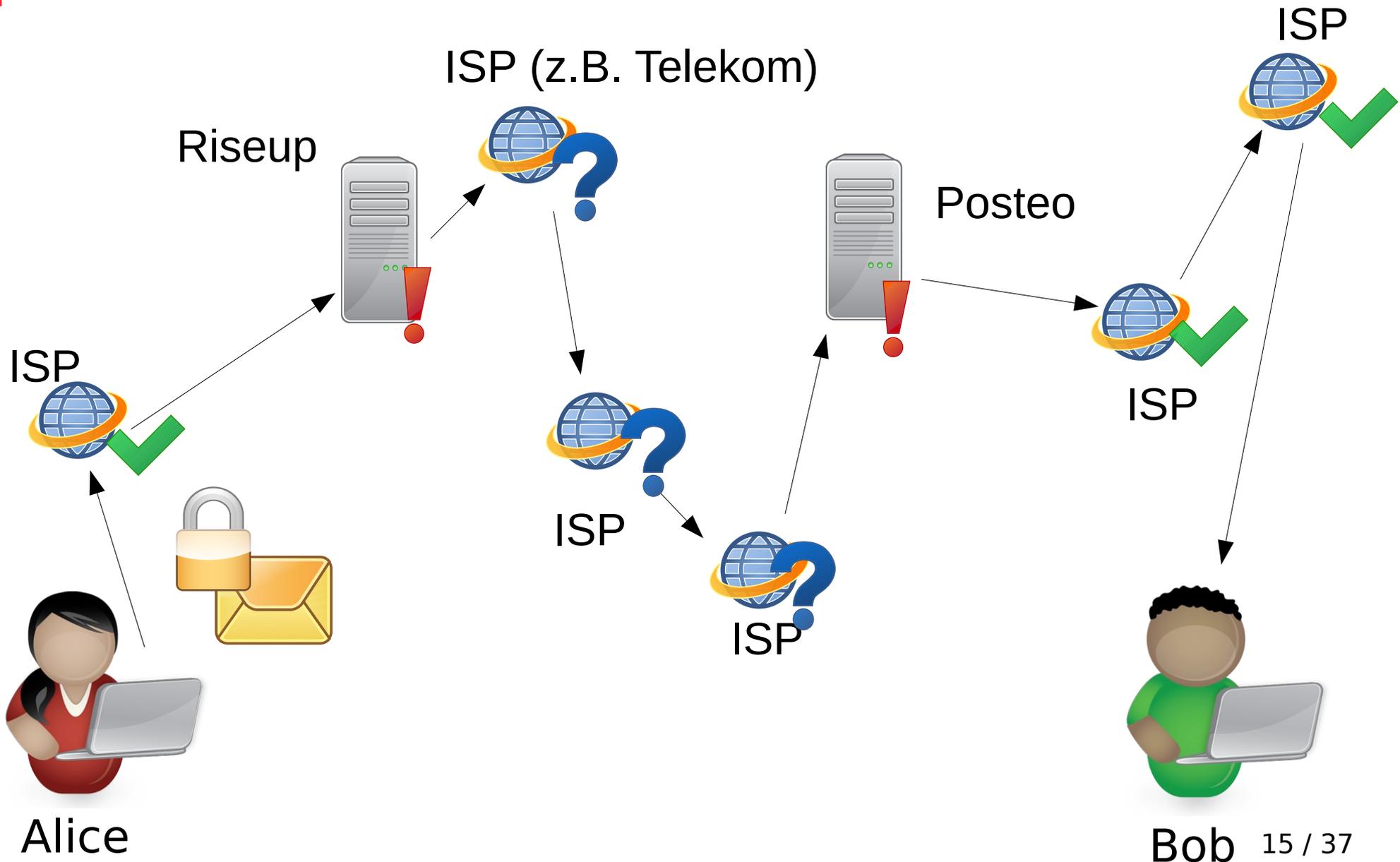


# Transportverschlüsselung

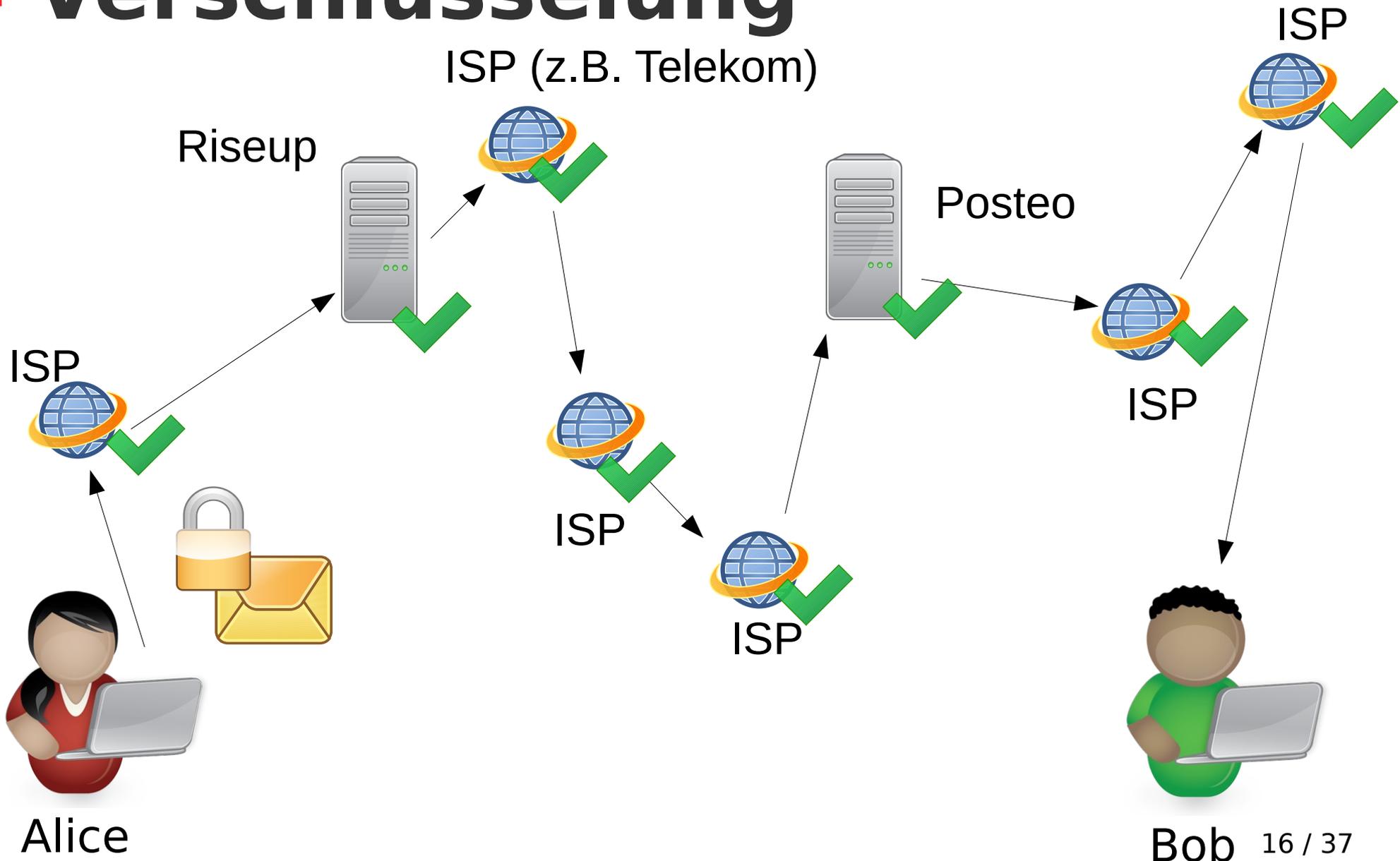
- Transportverschlüsselung ist weit verbreitet
  - SSL/TLS
  - STARTTLS



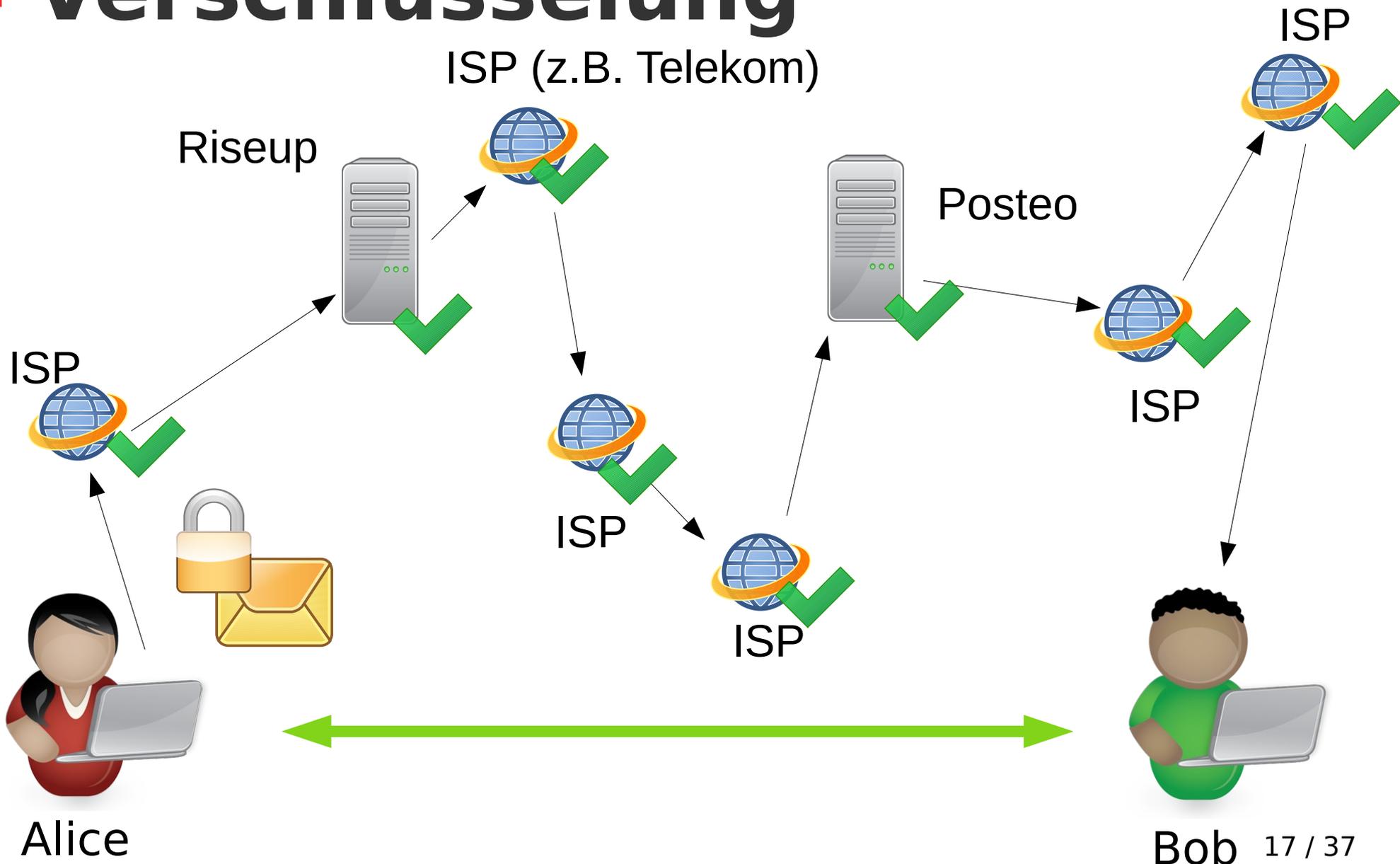
# Transportverschlüsselung



# Ende-zu-Ende-Verschlüsselung



# Ende-zu-Ende-Verschlüsselung





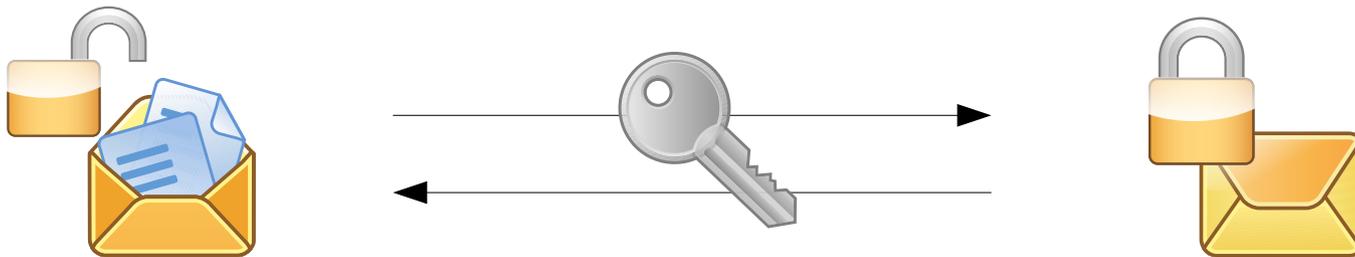
# Ende-zu-Ende- Verschlüsselung

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

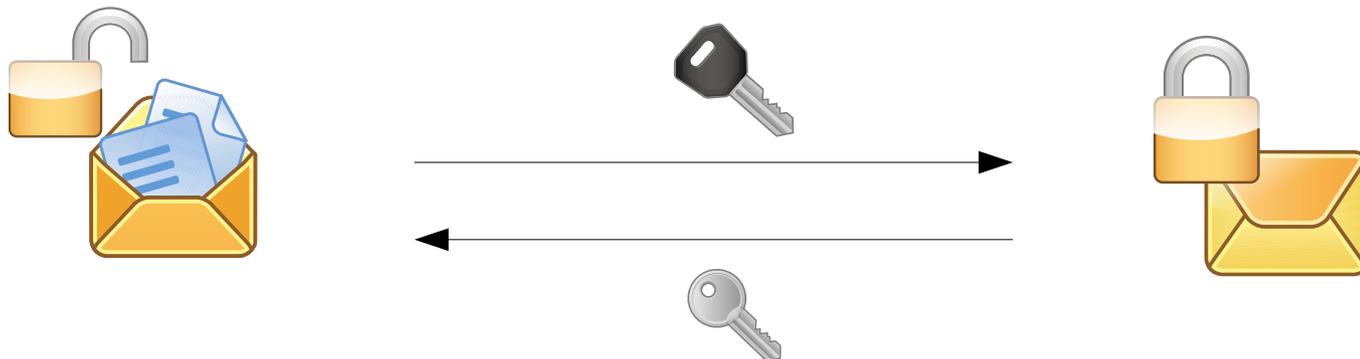
# Verschlüsselung!

- Grundprinzipien:

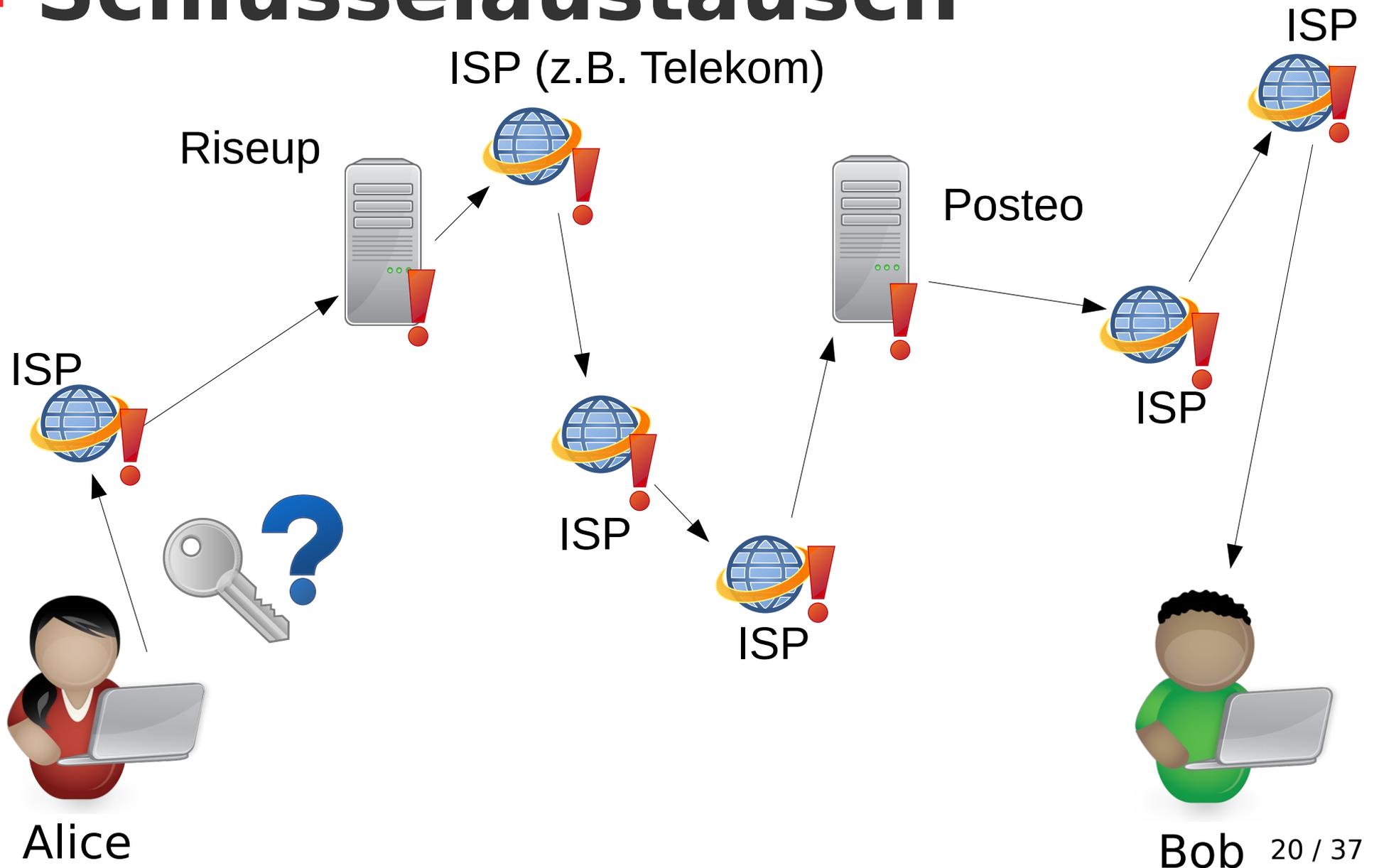
- **Symmetrische Verschlüsselung**



- **Asymmetrische Verschlüsselung**

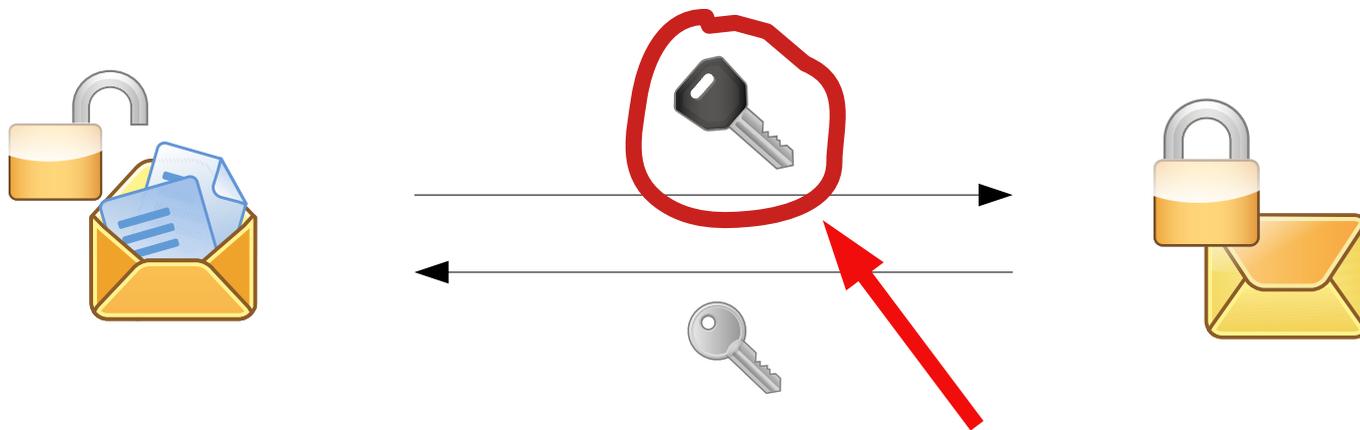


# Problem: Schlüsselaustausch



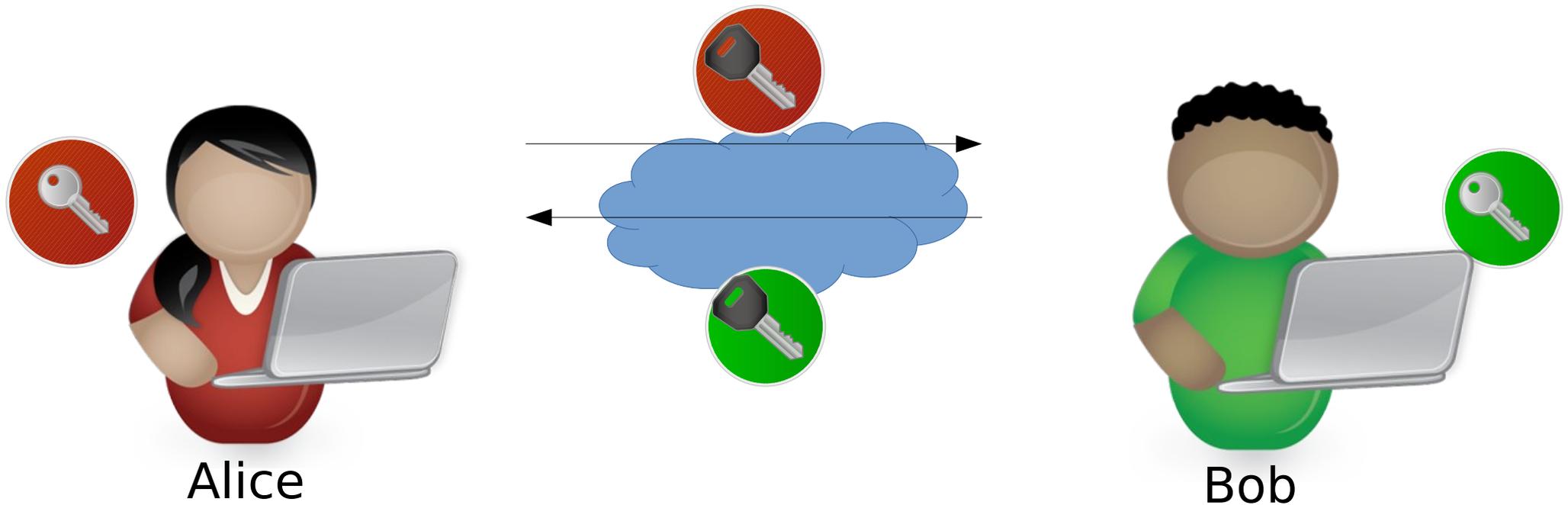
# Problem: Schlüsselaustausch

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

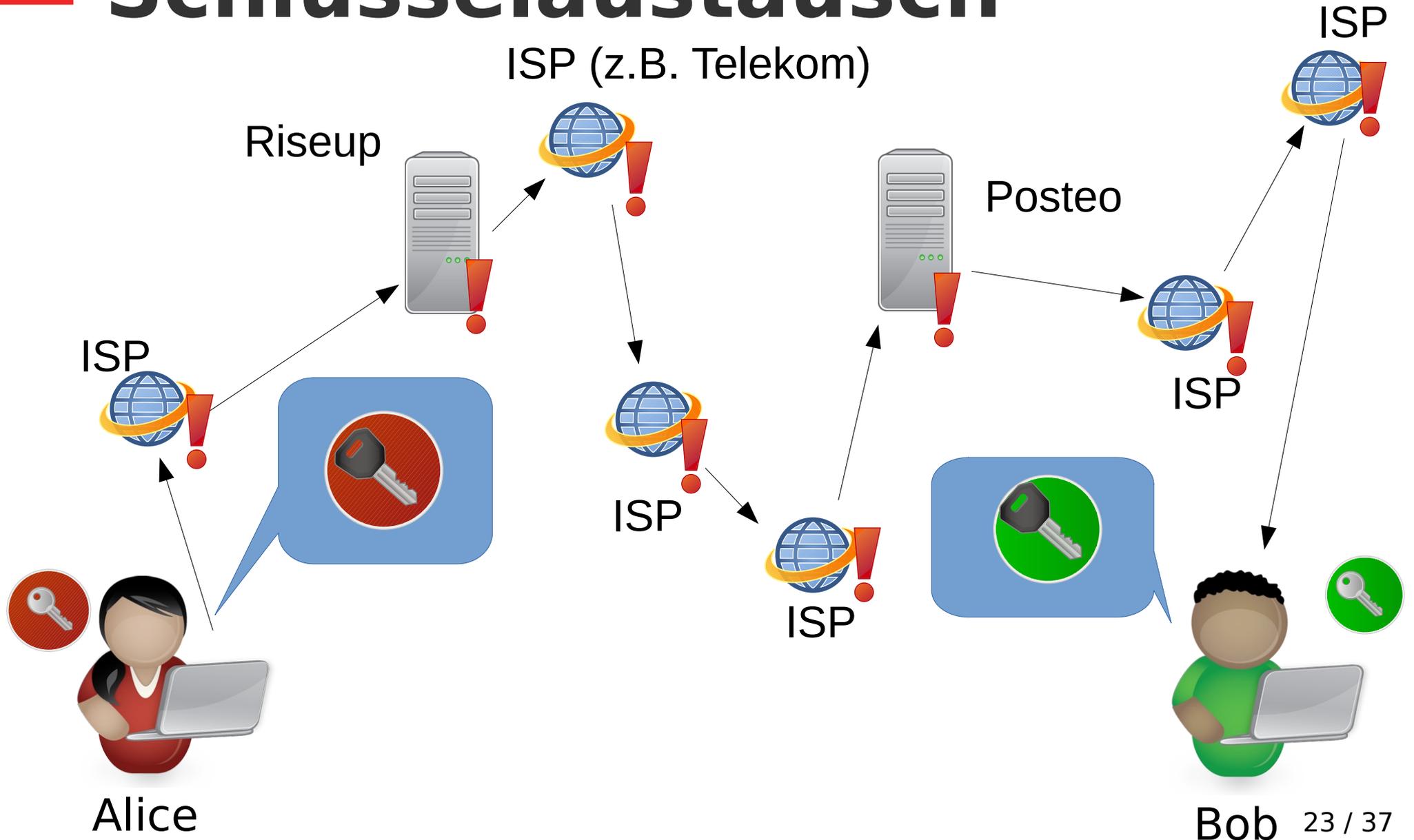


Ich kann diesen Schlüssel weitergeben!

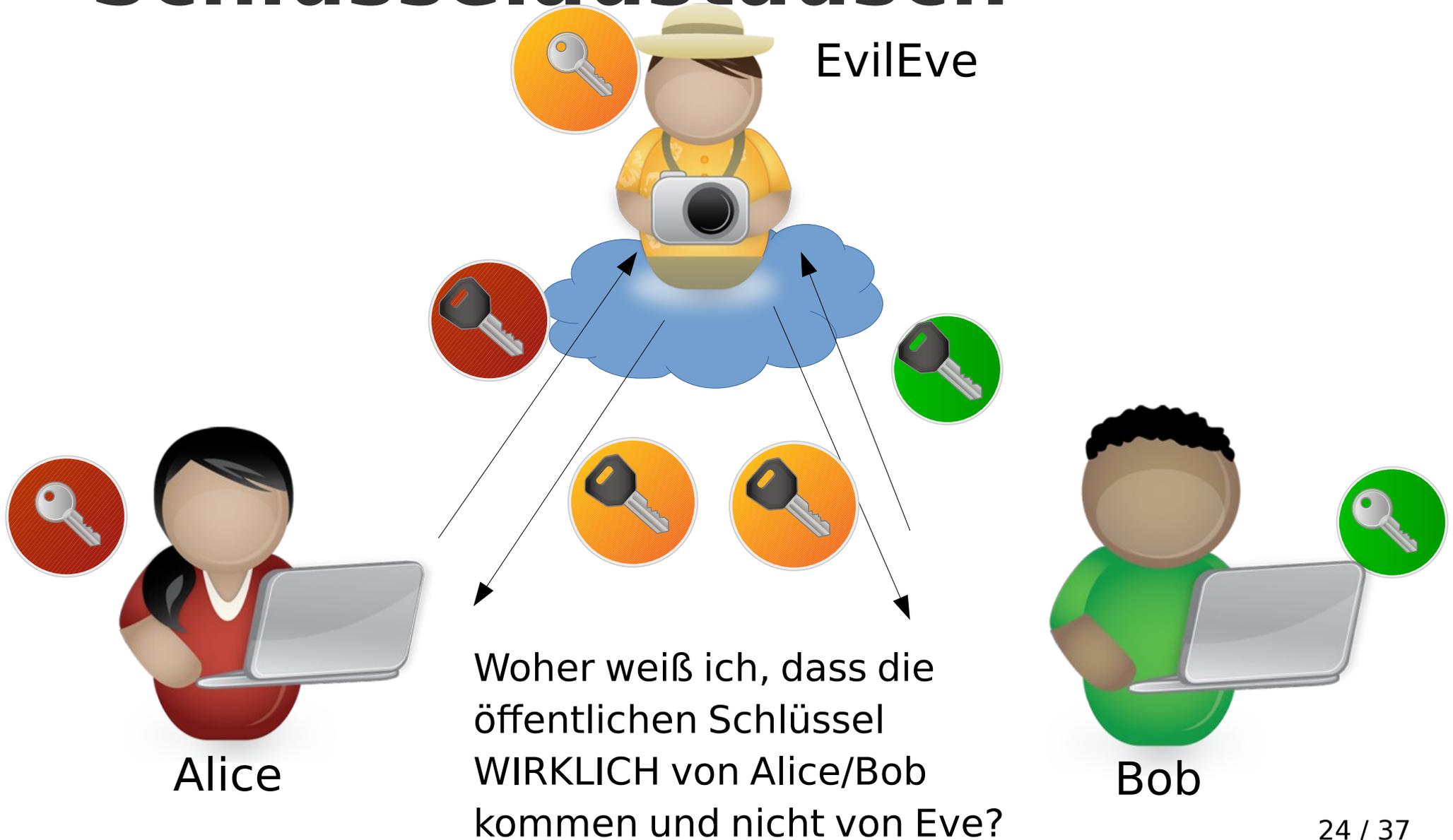
# Problem: Schlüsselaustausch



# Problem: Schlüsselaustausch



# Problem: Schlüsselaustausch



# 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 Schlüssel 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

The screenshot shows a WhatsApp chat window with the contact name 'vmann' circled in red. The chat contains two images of SpongeBob SquarePants. The second image is a meme with the text 'Spong · über giphy.com'. Below the images, there is a timestamp '21:50 · Zugestellt'. At the bottom of the chat, there is a text input field with the placeholder 'TIPPE EINE NACHRICHT'. To the right of the chat, there is a 'DETAILS' tab and a 'GERÄTE' (Devices) section. The 'GERÄTE' section lists three devices: 'HANDY' (circled in red) with ID 'F6 C4 18 F0 D2 5F 8A 00', 'DESKTOP-COMPUTER' with ID 'B2 7C 45 68 F5 2C 2A BE', and another 'DESKTOP-COMPUTER' with ID 'A3 56 C1 18 29 80 45 75'. At the bottom of the details panel, there is a 'GRUPPE ERSTELLEN' (Create Group) button.

vmann

vmann

@vmann

DETAILS GERÄTE

Wire gibt jedem Gerät einen einzigartigen Fingerabdruck. Vergleiche diese mit vmann und überprüfe deine Unterhaltung.

Warum Unterhaltungen überprüfen?

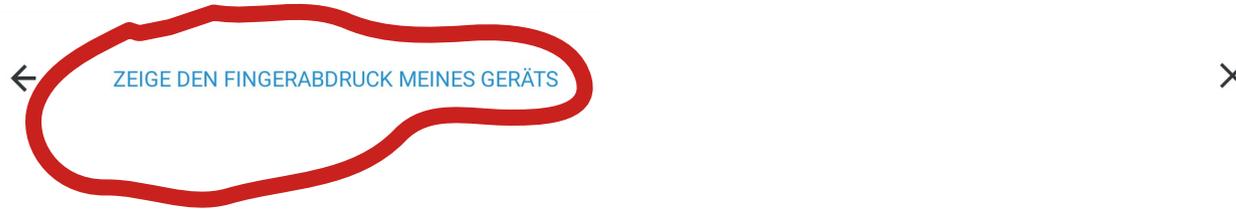
**HANDY**  
ID: F6 C4 18 F0 D2 5F 8A 00

**DESKTOP-COMPUTER**  
ID: B2 7C 45 68 F5 2C 2A BE

**DESKTOP-COMPUTER**  
ID: A3 56 C1 18 29 80 45 75

GRUPPE ERSTELLEN

# Beispiel: Wire Teil 2



Überprüfe, ob dieser Fingerabdruck mit dem auf vmann' Gerät übereinstimmt.  
[Wie mache ich das?](#)

**HANDY**  
ID: **F6 C4 18 F0 D2 5F 8A 00**

**6a 84 fa d5 ae 69 36 4a 94 77 2f e8 1f d5**  
**2c 53 b6 dd fe 50 10 45 73 e3 59 03 4f 74**  
**0b 2d 46 7e**

NICHT ÜBERPRÜFT [SESSION ZURÜCKSETZEN](#)

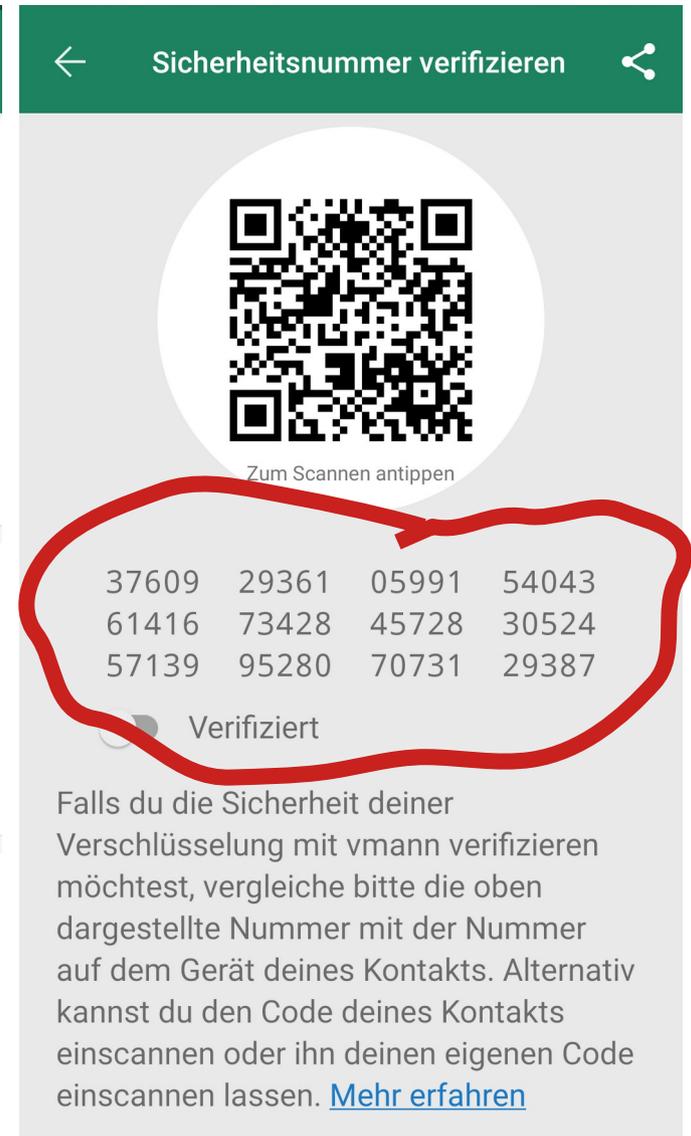
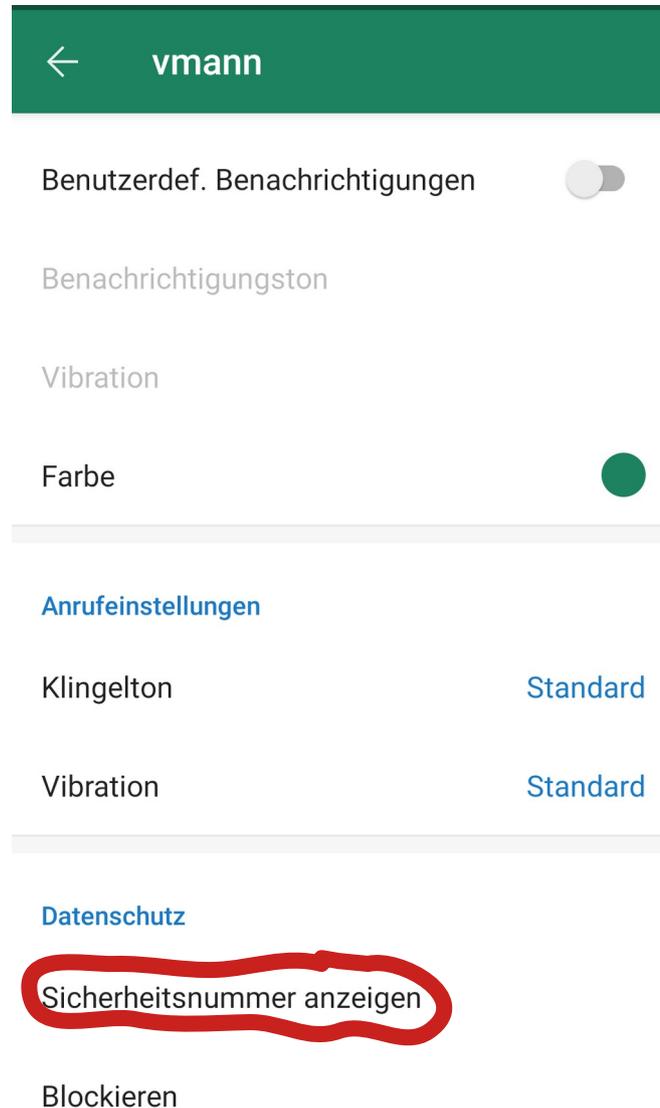
Geräte-Fingerabdruck

**HANDY**  
ID: **D0 44 B0 B2 C7 B4 C5 AE**

**ea cb b3 fa a8 62 58 74 9a c4 12 44 d0 e9**  
**37 27 03 21 79 f8 53 7e 48 ba f9 29 4b 45**  
**d9 b9 e4 3e**

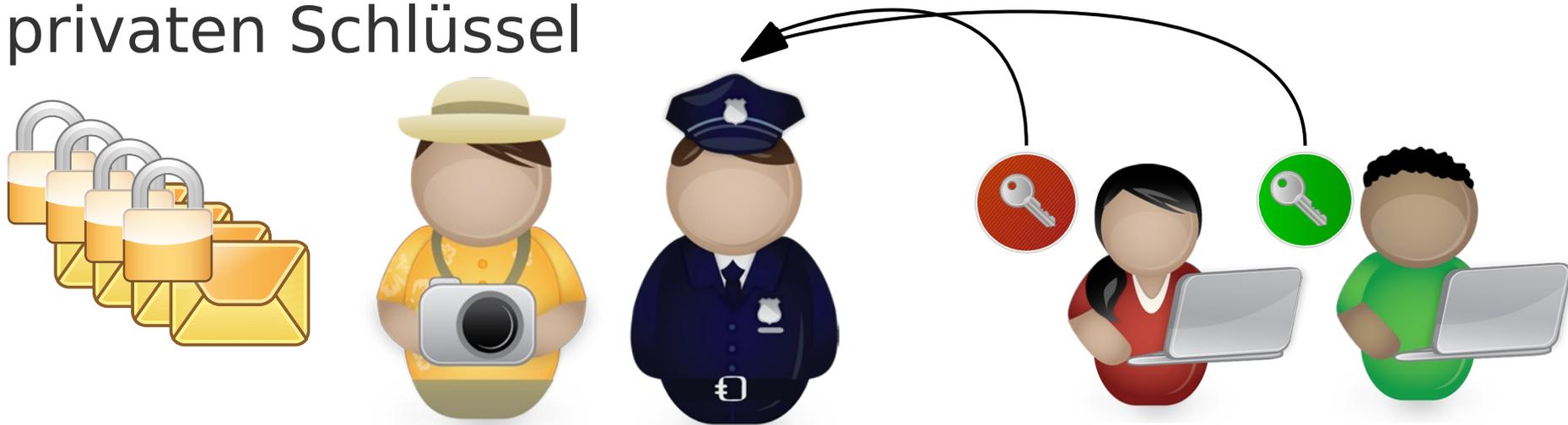
[ALLE MEINE GERÄTE ANZEIGEN](#)

# Beispiel: Signal



# Forward Secrecy

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

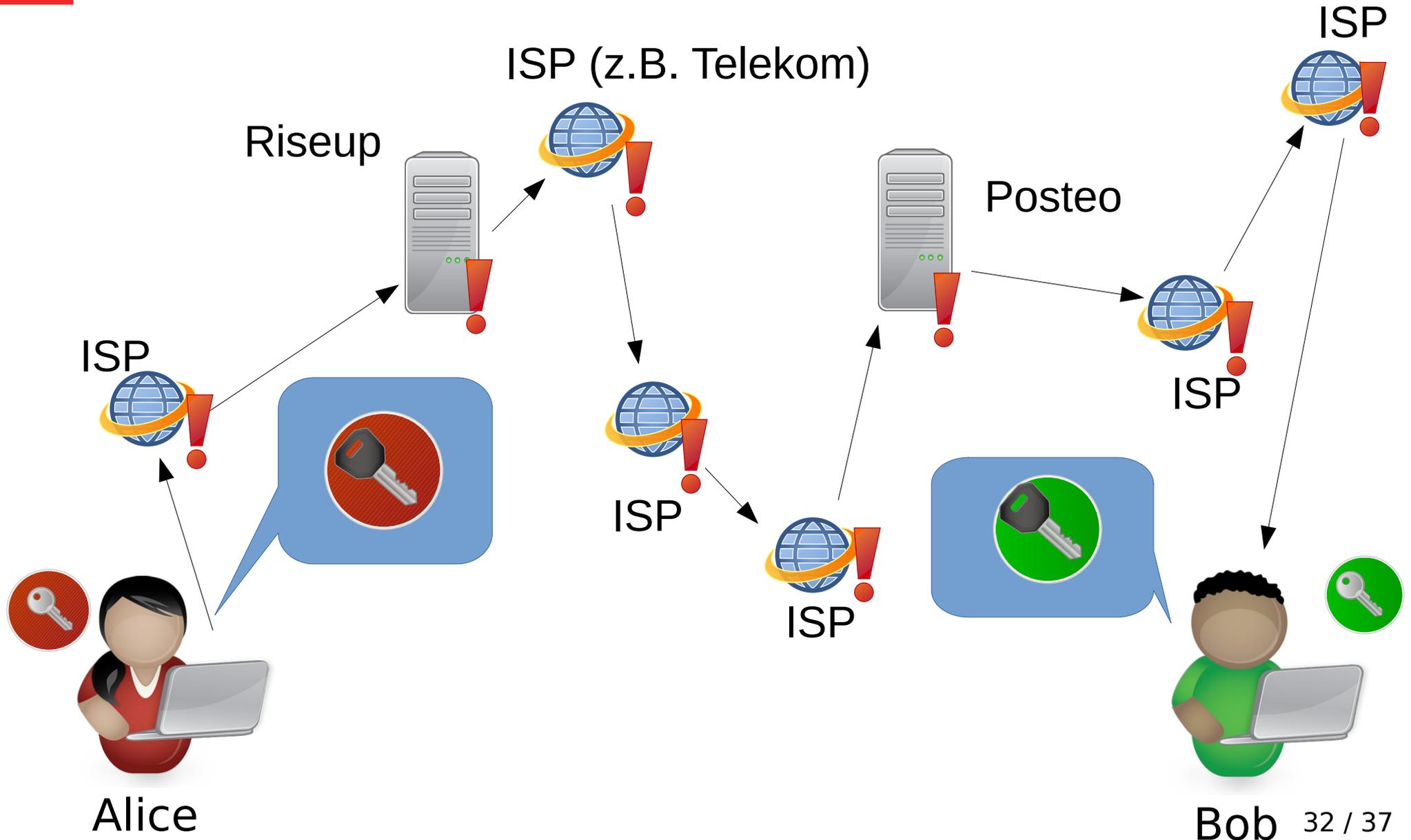


- Lösung: neue Schlüssel pro Nachricht
- Implementiert in Signal/Wire/OMEMO, aber **nicht** in PGP

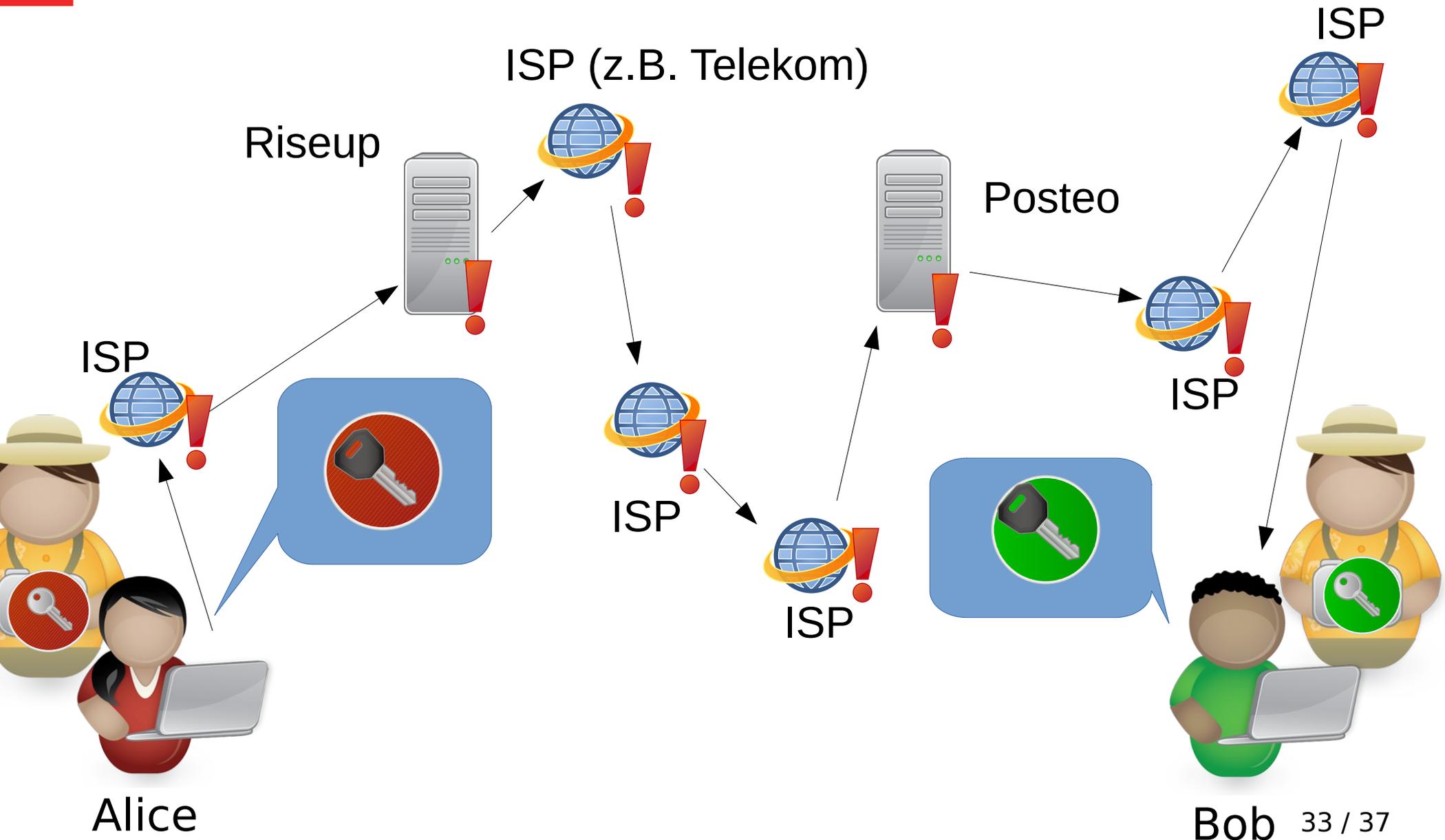
# Grenzen der Ende-zu-Ende-Verschlüsselung

- 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 sog. “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?