Überwachungsstaat vs Bürgerrechte

Die europäische Data Retention Richtlinie

lukas.feiler@lukasfeiler.com
http://www.lukasfeiler.com

Die Richtlinie und die nationalen Umsetzungen

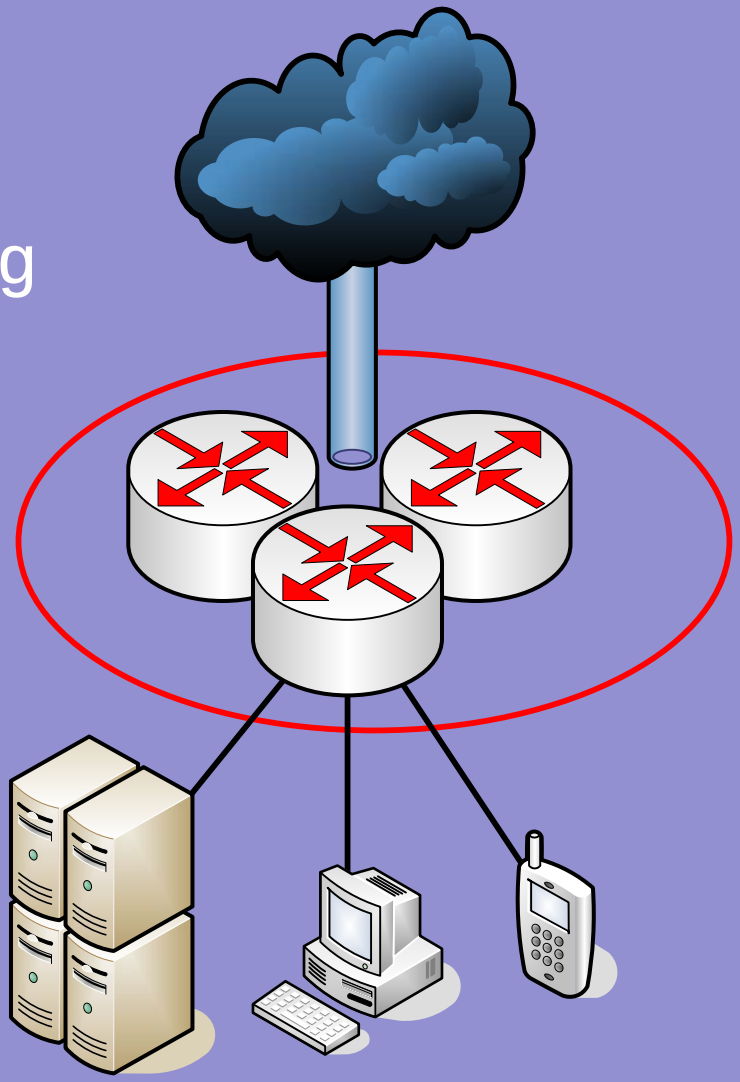
1) Speicherpflichtige Unternehmen
2) Auf Vorrat zu speichernde Daten
3) Speicherfrist
4) Zugriff auf Vorratsdaten
5) Kostentragung

Umgehungsmöglichkeiten

Speicherpflichtige Unternehmen:

RL: ausschließlich
- **Netzbetreiber** (Infrastruktur)
- **Access Provider** (Datenübertragung ins Telefonnetz/Internet)

Nicht:
- Hosting Provider
- Betreiber einer Website
- Betreiber eines Gästebuches
- ...



Speicherpflichtige Unternehmen:

AT: nur Netzbetreiber & Access Provider
DE: nur Netzbetreiber & Access Provider
UK: nur Netzbetreiber & Access Provider
FR: Netzbetreiber, Access Provider und
alle Betreiber von Online-Diensten, die eine interaktive Kommunikation ermöglichen

Auf Vorrat zu speichernde Daten:

Nach der Richtlinie und in AT, DE & UK:
Verkehrs- und Standortdaten betreffend 5 Bereiche:

- a) Telefonnetz
- b) Mobilfunk

} Umzusetzen bis Sept 2007

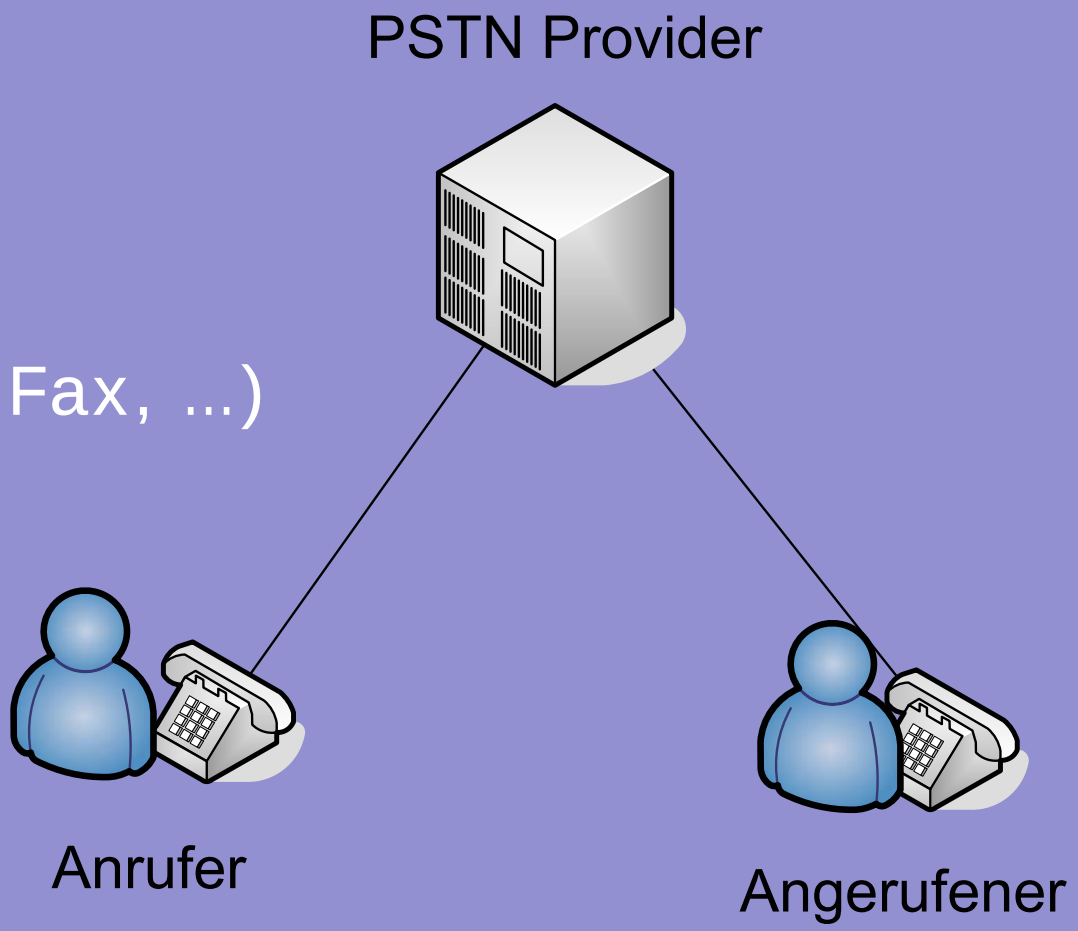
- c) Internet-Zugang
- d) E-Mail
- e) VoIP

} Umzusetzen bis März 2009

Keine Inhaltsdaten

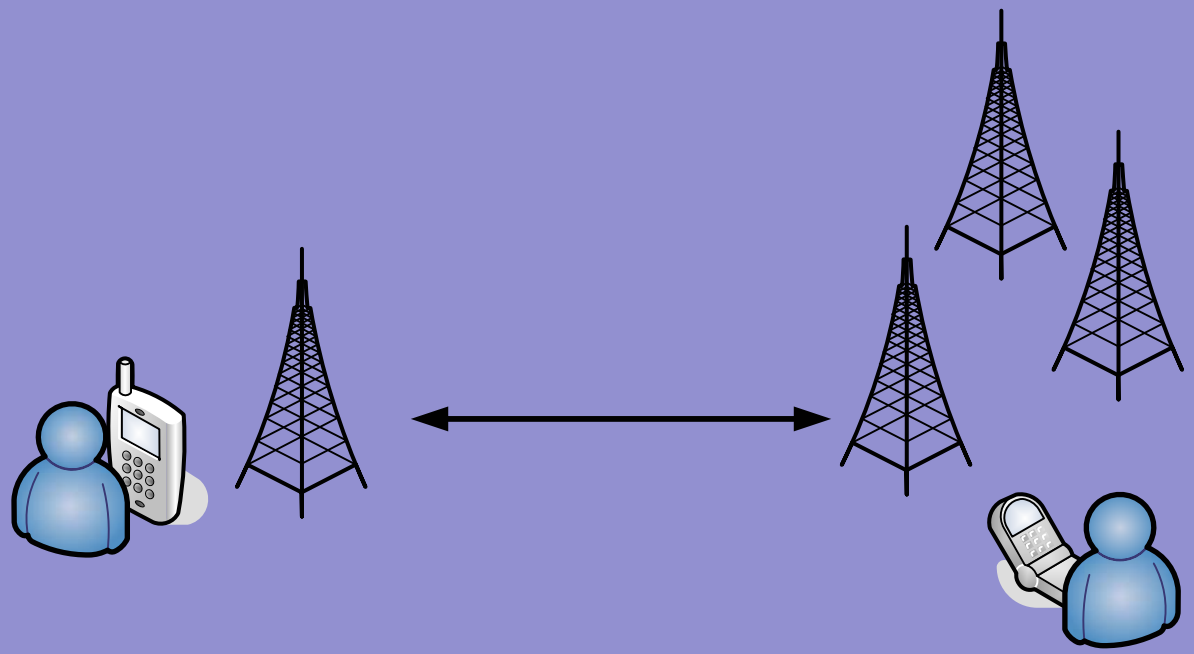
Telefonnetz

- Für beide Kommunikationspartner
  - Rufnummer
  - Name
  - Anschrift
- Beginn & Ende
- Telefondienst (Anruf, SMS, Fax, ...)



Mobilfunk

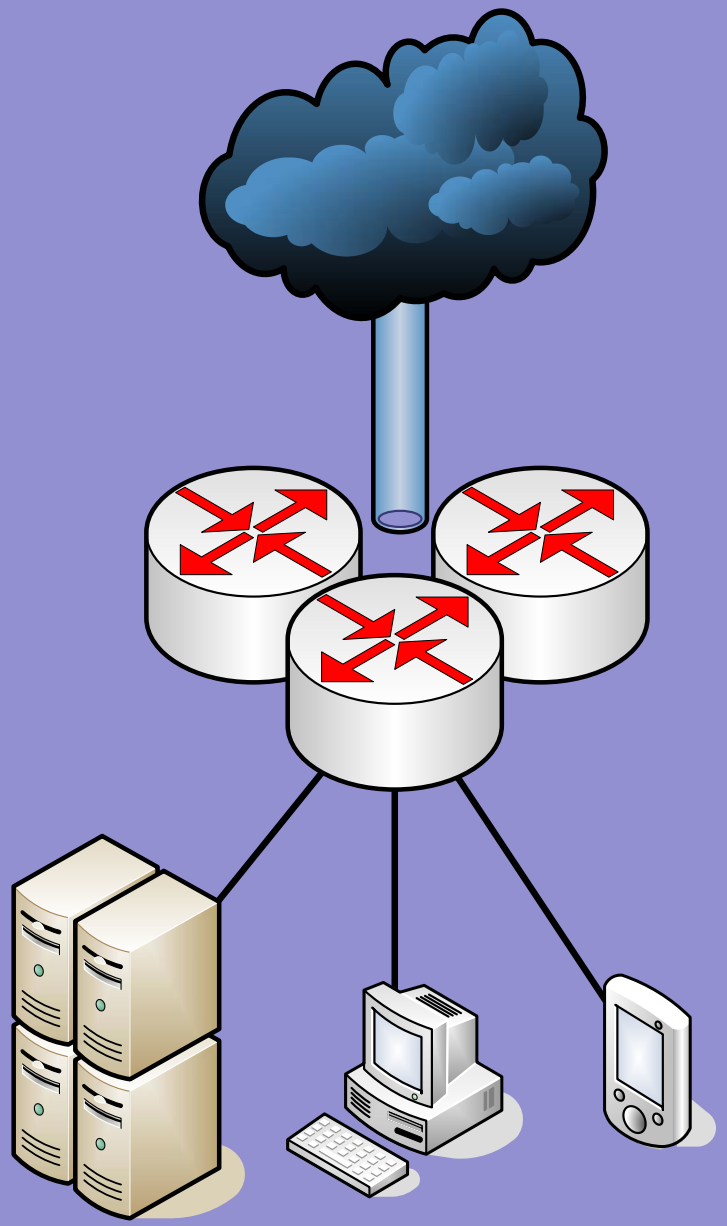
- Für beide Kommunikationspartner
  - Rufnummer
  - Name
  - Anschrift
  - IMSI & IMEI
- Beginn & Ende
- Telefondienst
- Cell-ID



Wirkungsbereich eines Handy-Mastes in Wien: ca 100m Radius
vgl. http://www.senderkataster.at/

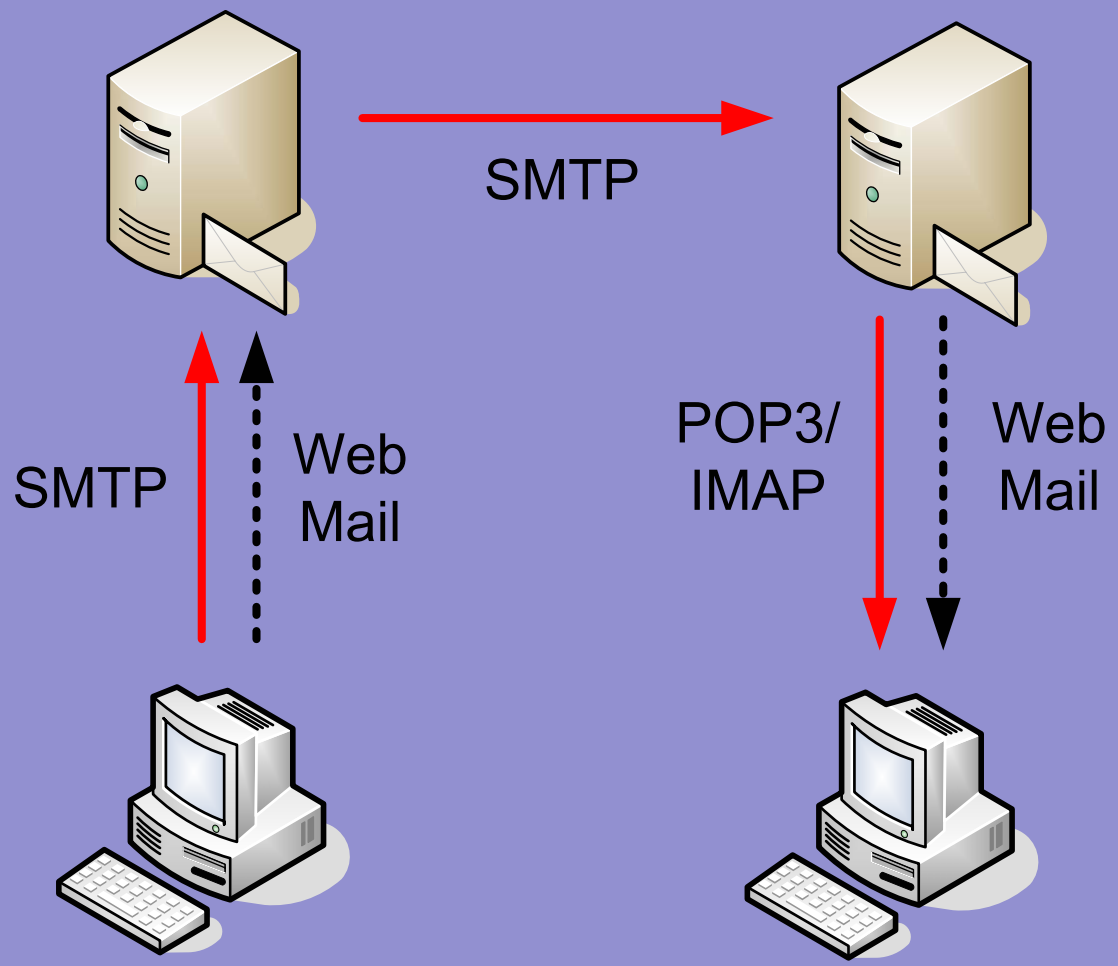
Internet-Zugang

- IP-Adresse
- Name
- Anschrift
- Beginn & Ende
- Endeinrichtung (zB Rufnummer)
- Cell-ID bei mobilen Geräten



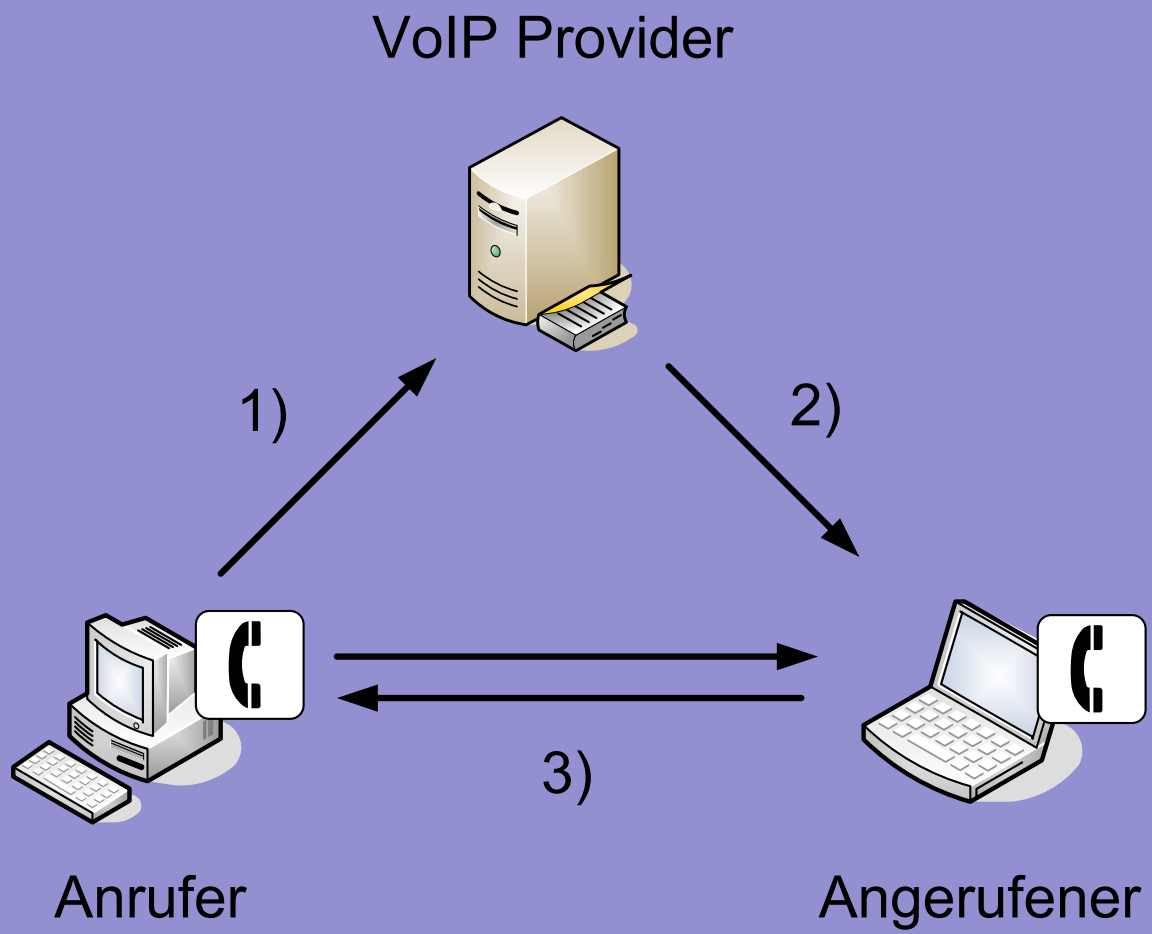
E-Mail

- Für beide Kommunikationspartner
  - Name
  - Anschrift
  - E-Mail-Adresse
  - IP-Adresse
- Zeitpunkt
- Cell-ID bei mobilen Geräten



VoIP

- Für beide Kommunikationspartner
  - Name
  - Anschrift
  - VoIP-Adresse
  - IP-Adresse
- Zeitpunkt
- Cell-ID bei mobilen Geräten



Grenzen der Vorratsdatenspeicherung:

Grundsätzlich darf nur gespeichert werden, was in eine der 5 – in der RL genannten – Kategorien fällt.

Daher nicht erfasst:

- WWW: auch Web-Mail
- Instant Messaging
- Newsgroups (RFCs 977, 1036)
- IRC – Internet Relay Chat
- P2P

sehr bedenkliche Ausnahmen in FR geplant: ua Benutzernamen, Passwörter & Nicknames

Die Speicherfrist

RL: 6 Monate bis 2 Jahre

AT: 6 Monate (BMI hätte gerne 1 Jahr)
DE: 6 Monate
UK: 1 Jahr
FR: 1 Jahr

3) Wie lange sind Vorratsdaten aufzubewahren?

Zugriff auf Vorratsdaten:

RL: zur Ermittlung, Feststellung und Verfolgung von „schweren Straftaten“

AT: Gerichtsbeschluss && Verdacht einer Straftat > 1 Jahr Freiheitsstrafe

DE: Gerichtsbeschluss && Verdacht einer mittels Telekommunikation begangenen Straftat
Jedoch: uU auch Übermittlung an BND & MAD

UK: alle Strafverfolgungsbehörden (ohne Richter!)
(Sect. 22(4) Regulation of Investigatory Powers Act 2000)
Voraussetzung: Verdacht einer Straftat

FR: Übermittlung nur mit Gerichtsbeschluss

Vorratsdaten: Übermittlung != Verarbeitung

Telco/
ISP

Name des
Verdächtigen

Alle Verkehrs- und
Standortdaten des
Verdächtigen

Law Enforcement
Agency

Telco/
ISP

Suchkriterien

Name des
Verdächtigen

Law Enforcement
Agency

4) Zugriff auf Vorratsdaten

Der Verdacht eine Straftat begangen zu haben

„warum sollte mich jemand verdächtigen, ich sprenge doch keine Häuser in die Luft …“

Ist auch nicht nötig:
§ 278b StGB: *„Wer sich als Mitglied an einer terroristischen Vereinigung beteiligt, ist mit […] bis zu zehn Jahren zu bestrafen.“*

Der Verdacht einer Terror-Absicht ist ausreichend.

Kostentragung

RL: N/A

AT: derzeit nicht vorgesehen
DE: kein Kostenersatz
UK: gänzlicher Kostenersatz
FR: kein Ersatz für Infrastruktur-Kosten

→ der Kunde bzw der/die SteuerzahlerIn kommen jedenfalls für die eigene Überwachung auf :)

Und wer zahlt dafür?

Anzahl der „lawful interception“ requests?

DE: ?
UK: ?

Anzahl der „lawful interception“ requests

DE: 35.329 (2006) + 460% seit 1998
UK: 351.243 (2005)
AT: ??.???

Quellen:
- DE: Pressemitteilung der deutschen Bundesnetzagentur vom 26. April 2007, http://www.bundesnetzagentur.de/media/archive/9712.pdf
- UK: Report of the Interception of Communications Commissioner for 2005-2006, http://www.official-documents.gov.uk/document/hc0607/hc03/0315/0315.pdf

Data Retention: Umgehungsmöglichkeiten

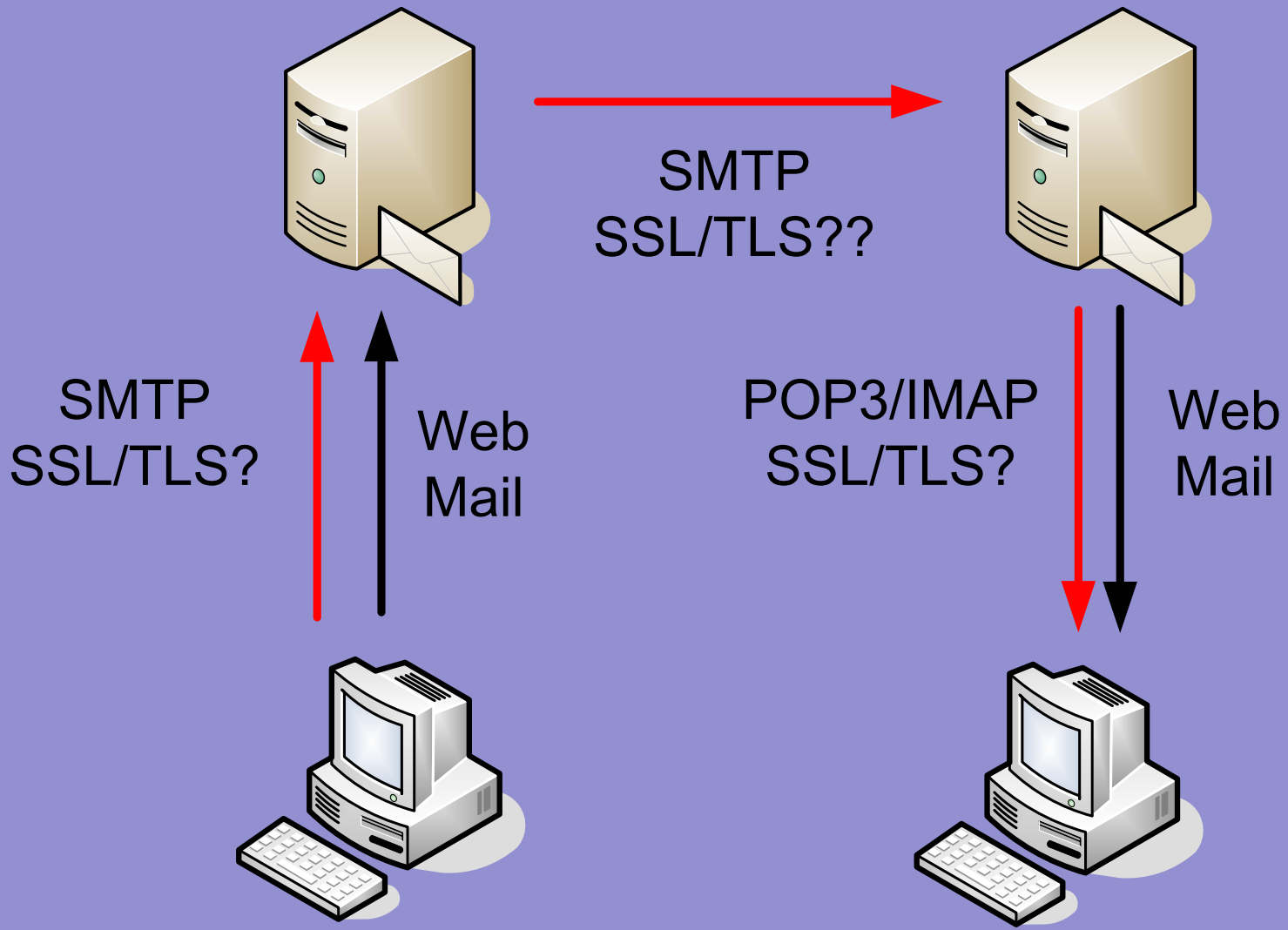
Im Bereich Festnetz- und Mobil-Telefonie:

- Wertkarten-Handys
  (Vorsicht: Cell-ID wird bei Erstaktivierung erfasst!)
- öffentliche Telefonzellen

Im Bereich Internet-Zugang, E-Mail & VoIP:

- Internet-Cafés
- öffentliche WLAN Hot-Spots
- WebMail: gmail, gmx & hotmail
- SMTP/POP3/IMAP over SSL/TLS
- VPNs
- SSH Tunnels (mittels SOCKS proxy)
- Tor

WebMail & SSL/TLS

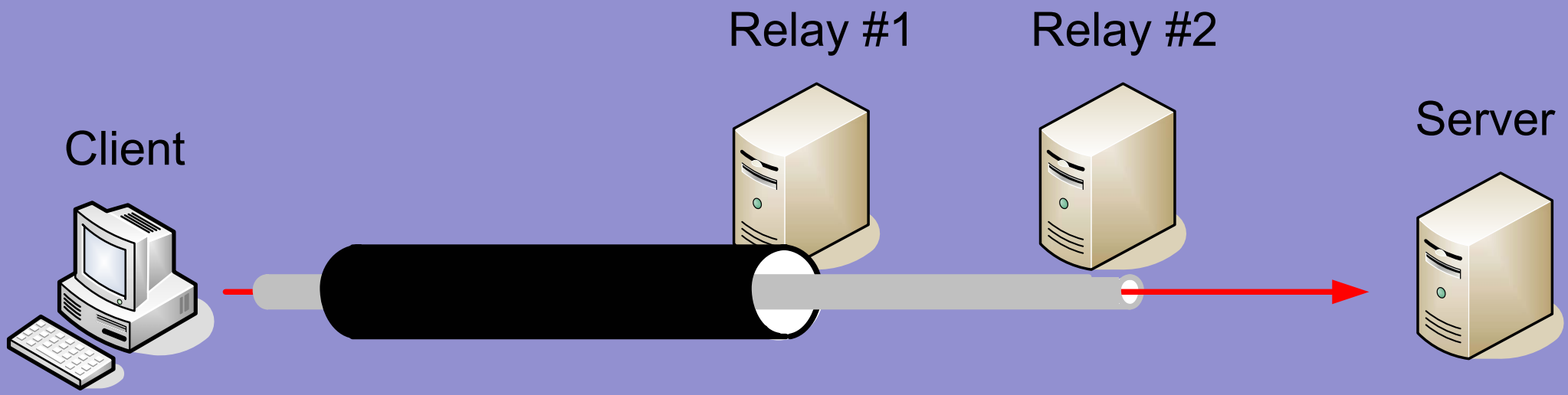


SSH Tunnels

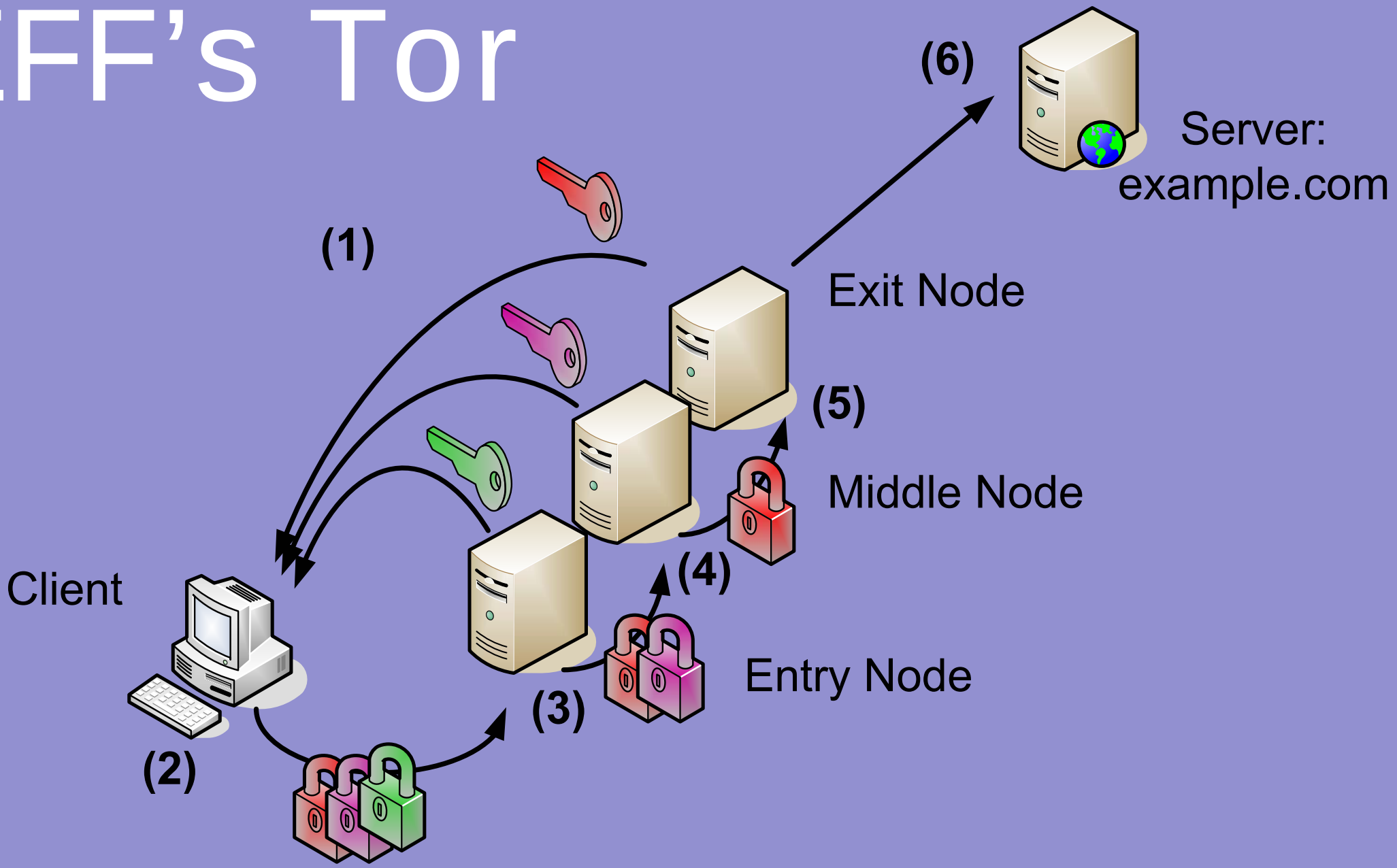
```
me@client $ ssh me@relay1 -L 2222:relay2:22
me@client $ ssh me@localhost -p 2222 -L 8080:server:80
me@client $ telnet localhost 8080
```

oder um relay2 als SOCKS proxy zu verwenden:

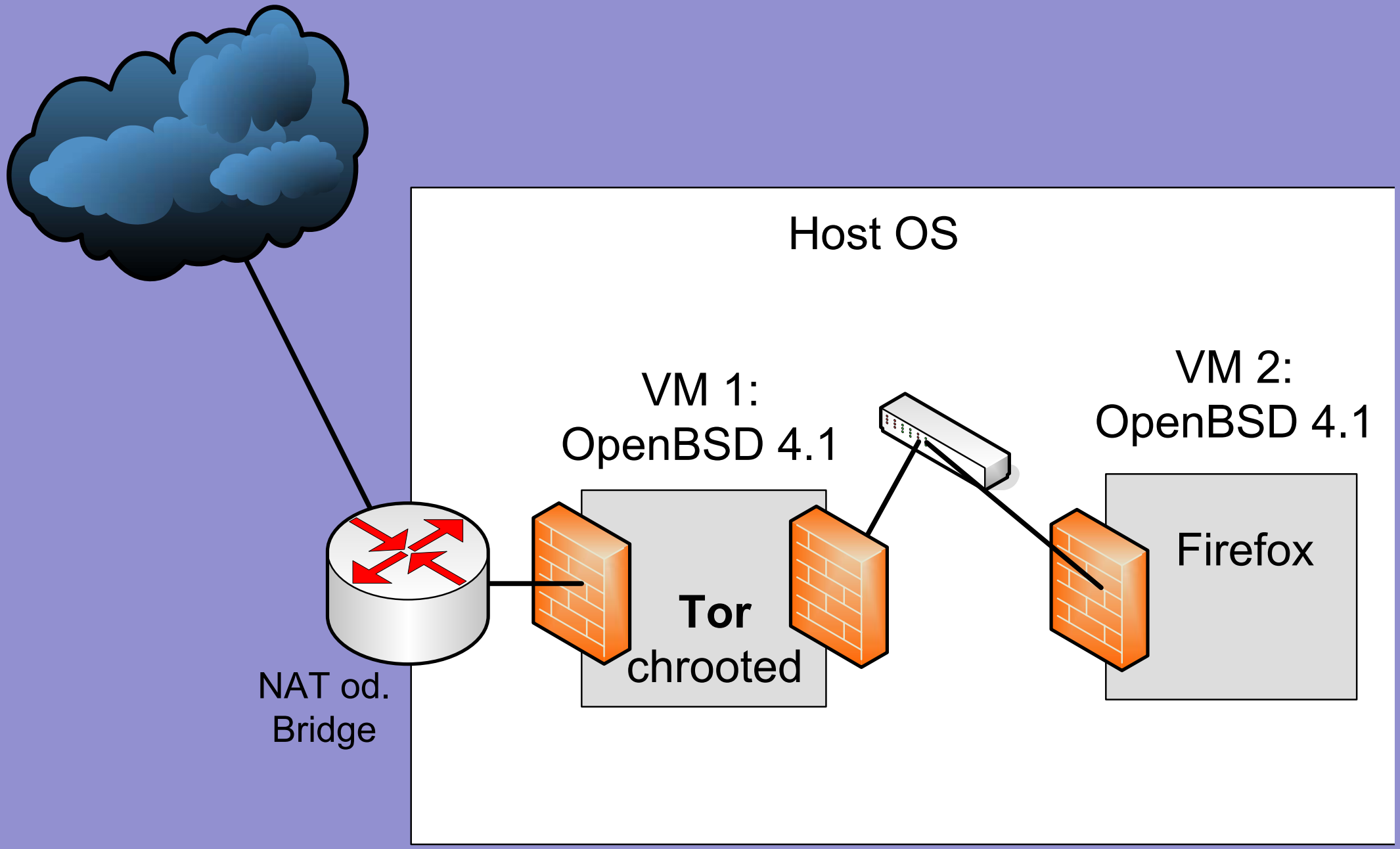
```
me@client $ ssh me@relay1 -L 2222:relay2:22
me@client $ ssh me@localhost -p 2222 -D localhost:3333
```



EFF's Tor



Umgehung: Tor



Ein mögliches Tor-Setup

Rechtliche Argumente gegen die Data Retention RL und ihre nationalen Umsetzungen

- Schwerer Eingriff in das Grundrecht auf Privatsphäre (Art 8 EMRK)
- Ist der Eingriff überhaupt geeignet das Ziel der Bekämpfung von Terrorismus und schwerer Kriminalität zu erreichen??

Formales Argument:
Die EG besitzt keine Gesetzgebungs-Kompetenz im Bereich des Strafrechts!

Filme zum Thema:

- Nineteen Eighty-Four (1984)
- Brazil (1985)
- The Conversion (aka Der Dialog; 1974)
- The Listening (2006)
- Das Leben der Anderen (2006)
- The Wire, Season 1 (HBO, 2002)
- Spying on the Home Front (PBS Fontline, 2007)
- The Enemy Within (PBS Fontline, 2006)

Privacy:
USE IT - OR LOSE IT
(as a society)!