Tor/Ökosystem LUG Frankfurt

1. Das Tor Project
2. Aufbau des Netzwerks
3. onion services im Überblick
4. Anwendungsszenarien im Überblick
5. Tor Metrics
6. Sicherheit im Allgemeinen
7. (Inter)national
8. Los geht‘s!

Was ist Tor?

Projekt

- **Tor Project, Inc, nonprofit Organisation**
- **Anonymisierung Verbindungsdaten**
- **Zensurfreiheit und Zensurresistenz**
- **Mitarbeitende im Projekt, Entwickler_innen, Community, Researcher, Node Operators, Onion-Service Operators, User**
- **Transparenz und Transparenzberichte**
- **viele weitere Projekte die verknüpft sind**

Aufbau des Netzwerks

Tor Directory Authorities (hardcoded in tor, 10 DA‘s, 5 müssen min. laufen, stellen zentralsten Punkt im Tor-Netzwerk dar)

Tor Knoten
- Guards (*“if Alice (the user) instead chose new relays for each circuit, eventually an attacker who runs a few relays would be her first andlast hop. With entry guards, the risk of end-to-end correlation for any given circuit is the same, but the cumulative risk for all her circuits over time is capped.“***)**
- Middle Relays
- Exit Relays
- flags (*z.B. verteilte Database an alle Relays mit HSDir flag für Introduction Points***)**

Tor Bridges (*nicht veröffentliche Relays, 2 Modi***)**

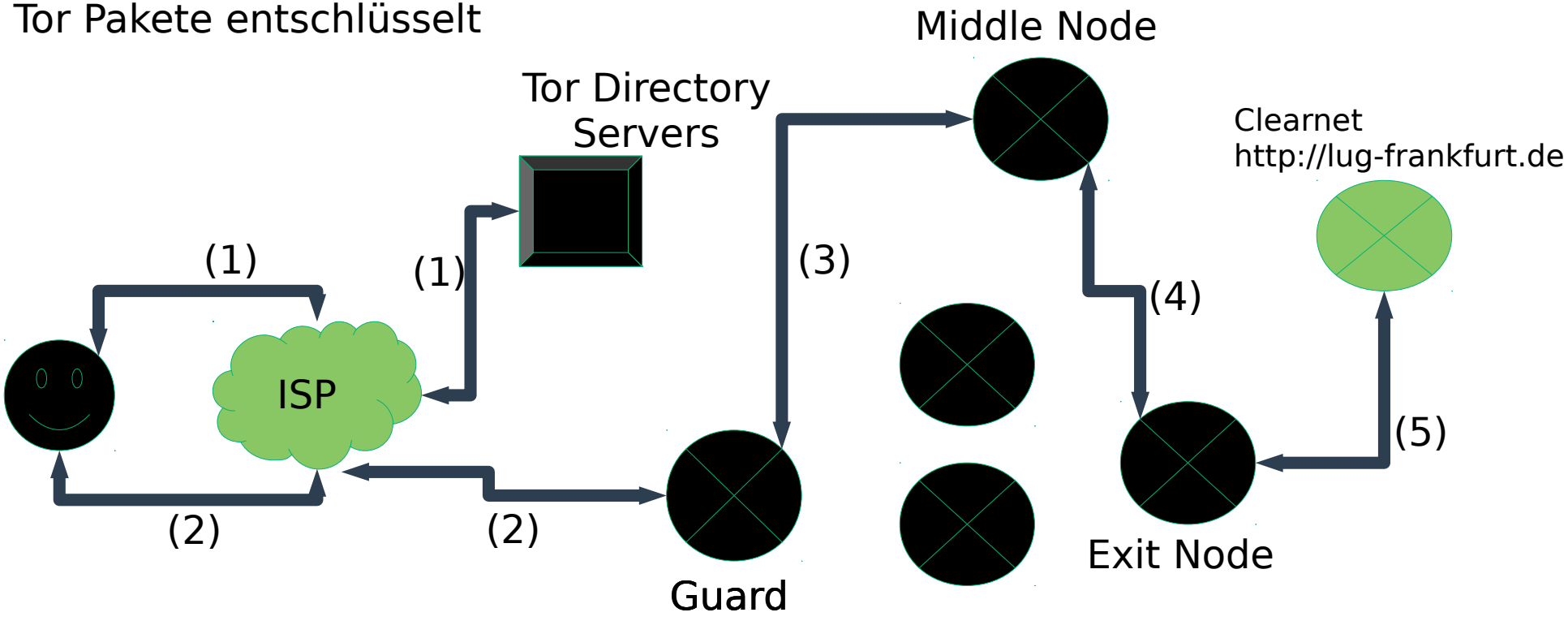
Onion Services Operators

Tor User

Aufbau des Netzwerks

Verbindung Standard

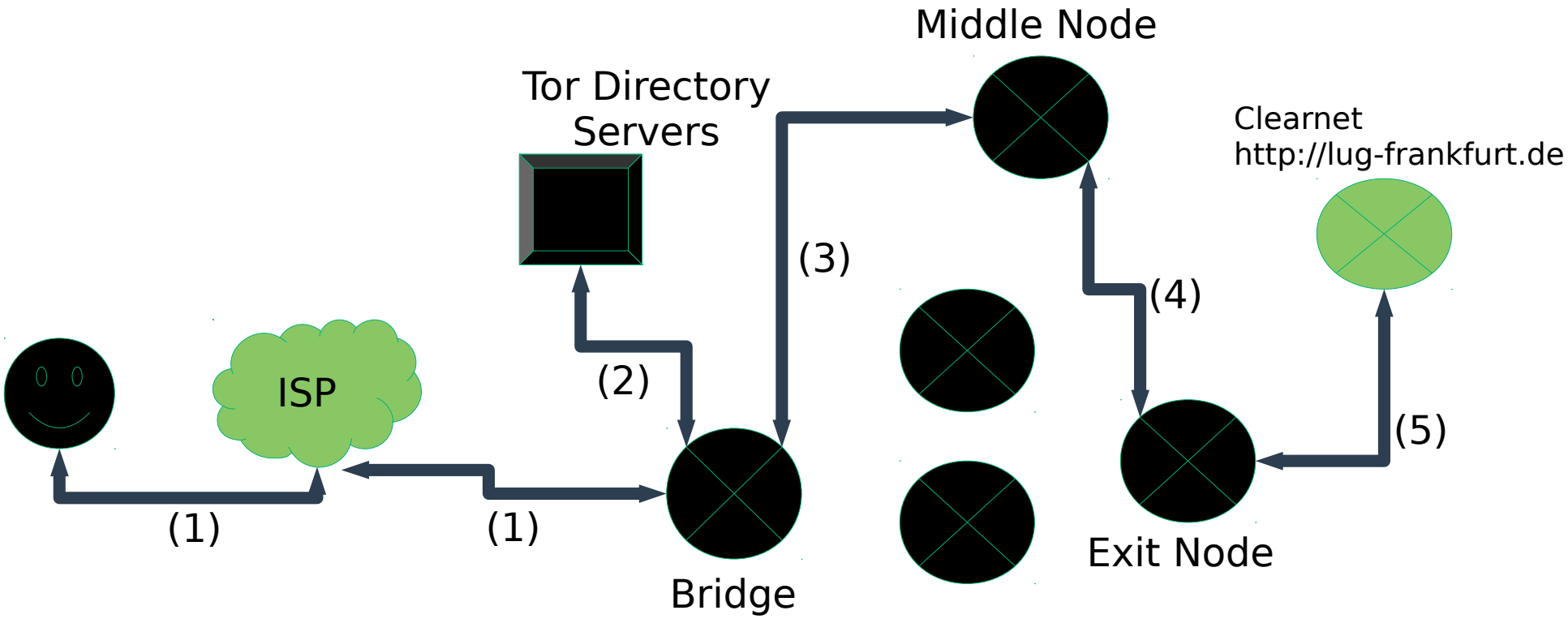
(1) Laden der aktuellen Liste aller Tor-Knoten
(2) „Zufällige“ Auswahl der Knoten für Route
(Tor Guard bleibt für eine gewisse Zeit der gleiche)
(3) Zum nächsten Knoten
(4) Zum nächsten Knoten
(5) Tor Pakete entschlüsselt



Aufbau des Netzwerks

Verbindung über Bridge

(1) Verbindung zur Bridge
(2) Über Bridge zu Tor Directory Servers
(3) Zum nächsten Knoten
(4) Zum nächsten Knoten
(5) Tor Pakete entschlüsselt

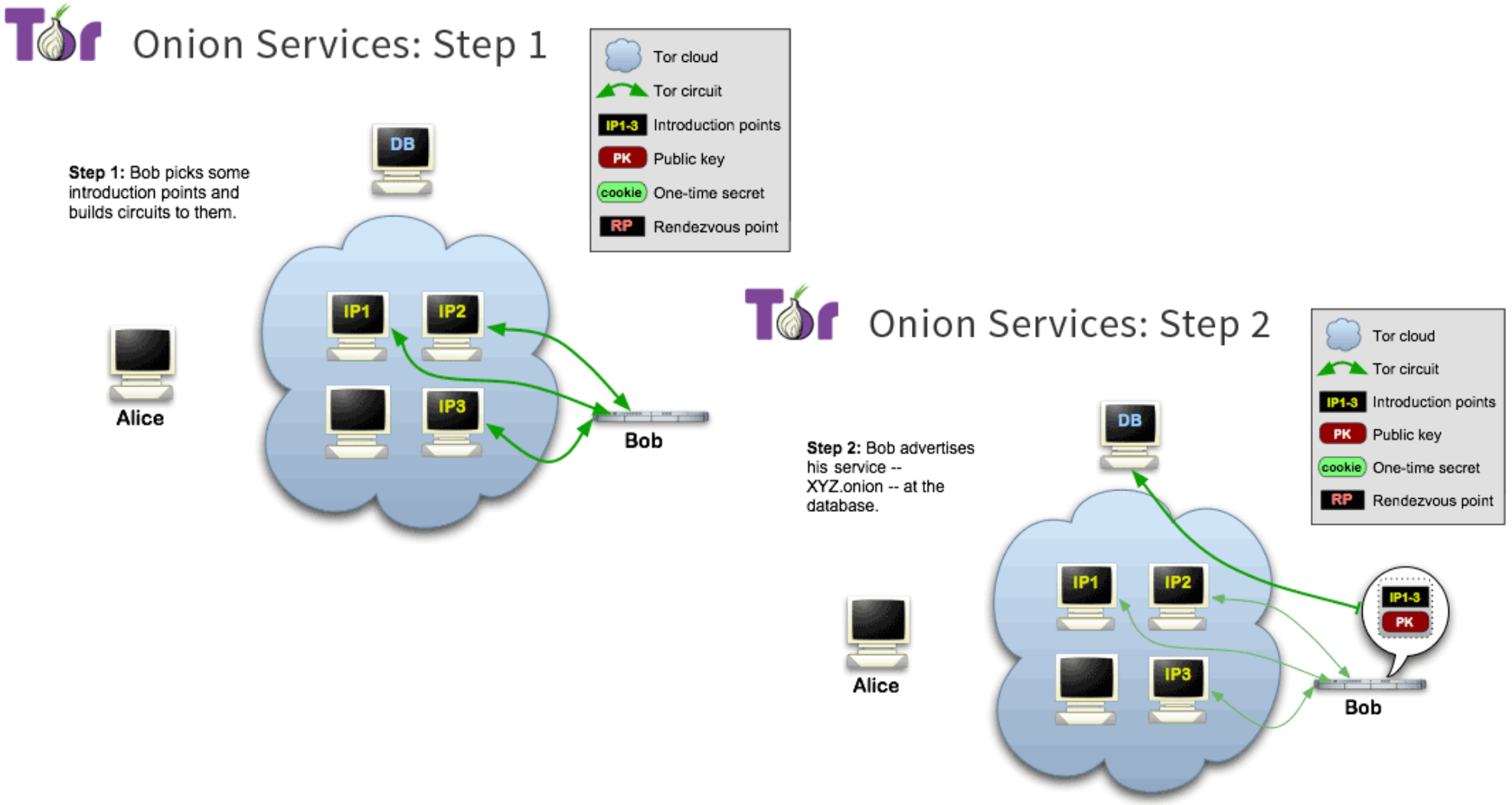


onion services im Überblick

- Dienste / Webseite die über das Tor Netzwerk erreichbar sind
- Standort und IP Adresse sind verdeckt
- Der gesamte Traffic ist Ende-zu-Ende verschlüsselt
- Die Adresse wird generiert (.onion) und stellt gleichzeitig den Public Key dar
- Keine Registrierung oder Anmeldung notwendig
- Kein Hoster, Domain-Seller etc. notwendig
- Es müssen keine Ports im NAT oder eigenen Location geöffnet werden
- Jeder Dienst kann ein Onion Service sein
- Kann und soll auch parallel betrieben werden

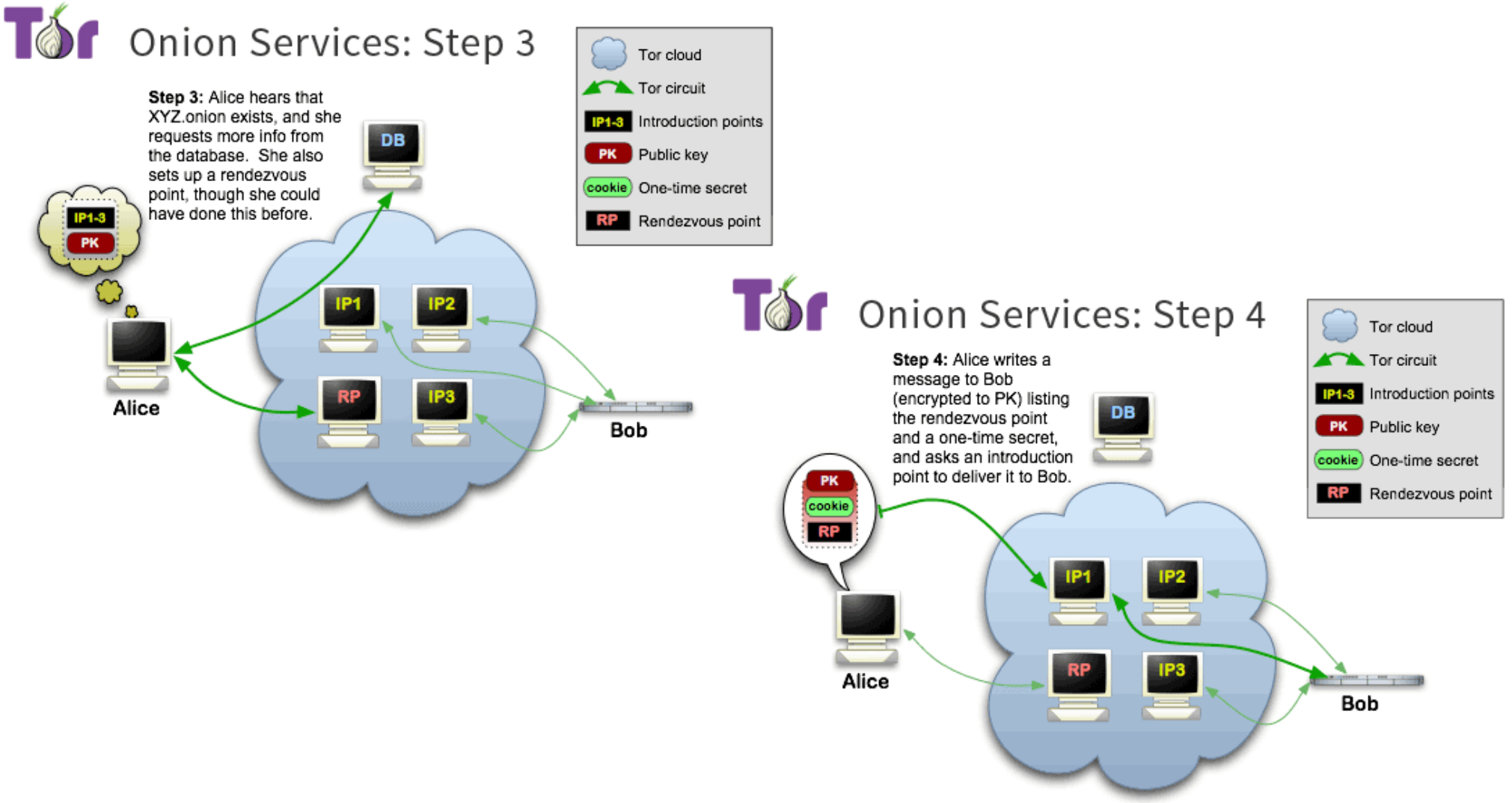
onion services im Überblick

Verbindung https://community.torproject.org/onion-services/overview/



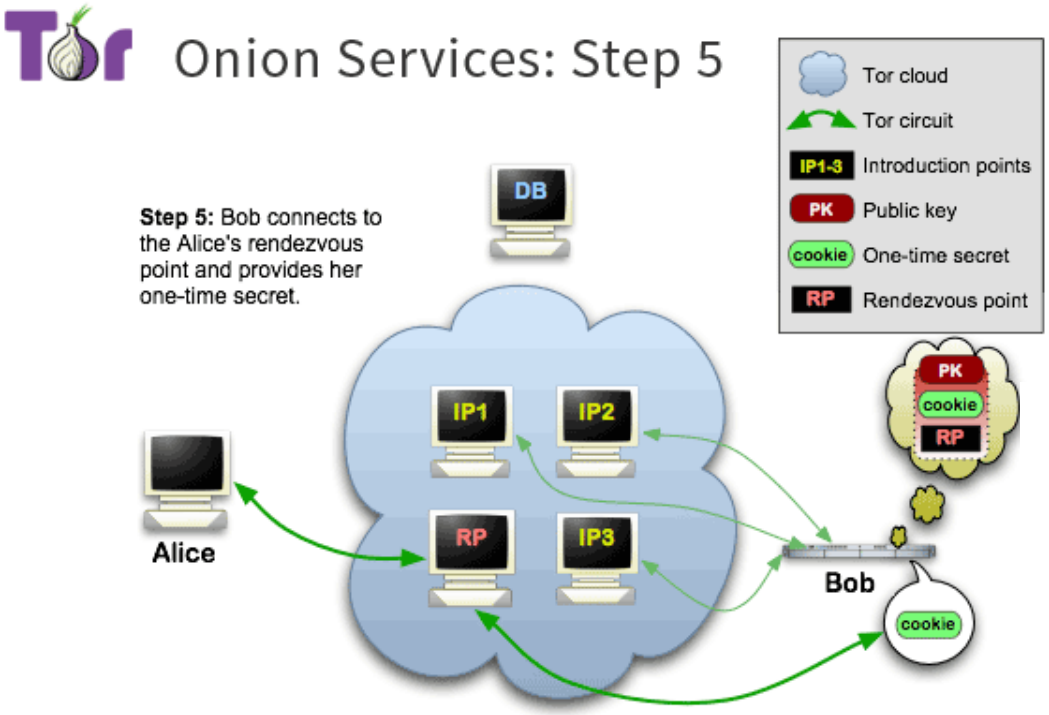
onion services im Überblick

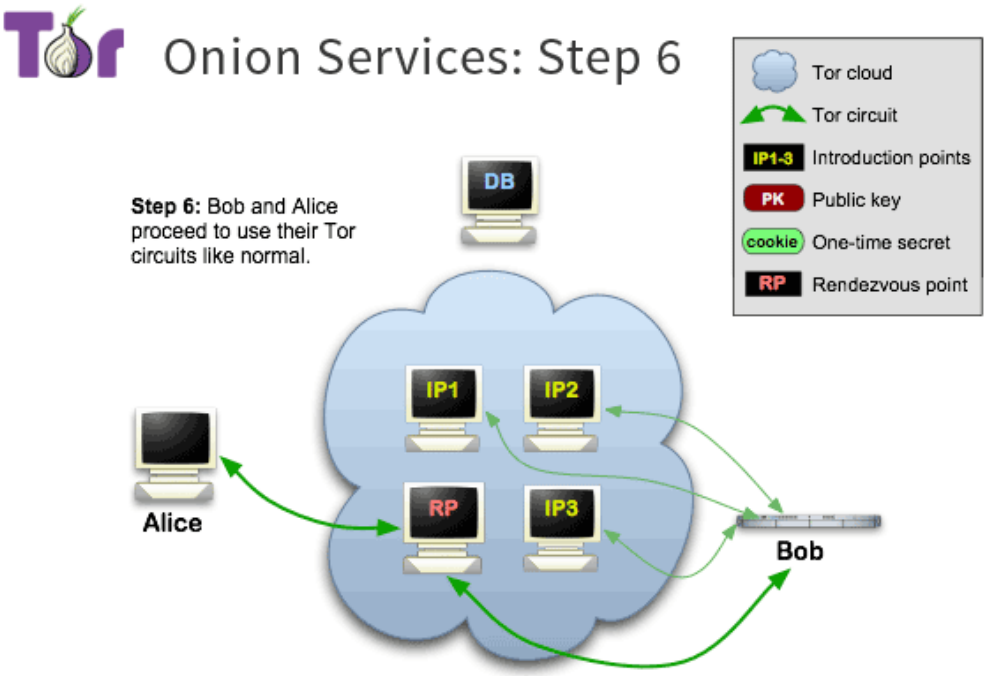
Verbindung https://community.torproject.org/onion-services/overview/



onion services im Überblick

Verbindung https://community.torproject.org/onion-services/overview/





Anwendungsszenarien im Überblick

Tor Browser

- angepasster Firefox (HTTPS-Everywhere + NoScript als Standard)

- startet tor Prozess (:9150)

- 3 Sicherheitsstufen

- div. Features

→ Anschauen und Probieren

Download immer prüfen

Anwendungsszenarien im Überblick

Tails

- Live Linux OS (Debian-basiert)
- zwingt alle Verbindungen über tor
- amnesic, überschreibt RAM beim Herunterfahren, div. Sicherheitsfeatures
- von DVD/CD, USB-Sticks, als VM zu starten (nicht empfehlenswert)
- große Menge an Privacy Tools on-board

Anwendungsszenarien im Überblick

Whonix

- Debian-basiert, Rolling-Release, nur noch eine Appliance
- zwei virtuelle Maschinen, Workstation+Gateway
- alle Verbindungen der Workstation werden aufs Gateway, damit über Tor gezwungen
- Workstation kennt nur Gateway
- sehr starke Trennung
- KVM, VirtualBox, QubesOS
- teilweise andere Anwendungsszenarien als Tails

Anwendungsszenarien im Überblick

Socks

- **torsocks** (Library for intercepting outgoing network connections and redirecting them through a SOCKS server)

  Beispiel *user@pc:~$ torsocks ssh root@217.217.217.1*

- **Proxy in div. Applikationen** (Messenger, Krypto-Wallets, apt-get, etc.)

- **tor als Anwendung auf Port 9050 mit Tor-Browser Port 9150**

Anwendungsszenarien im Überblick

OnionShare

- Dateien teilen, empfangen, minimale Webseite
- läuft als Onion Service
- sowohl GUI, als auch CLI
- einfache Benutzung

→ Anschauen und Probieren

Anwendungsszenarien im Überblick

Noch viele, viele mehr

- Briar Messenger (PlayStore)

- Orbot

- etc.

→ Anschauen und Probieren

Vorstellung Tor Metrics

Was ist es und was kann es?

“Users, advocates, relay operators, and journalists can better understand the Tor network through data and analysis made available by Tor Metrics.“

→ Anschauen und probieren

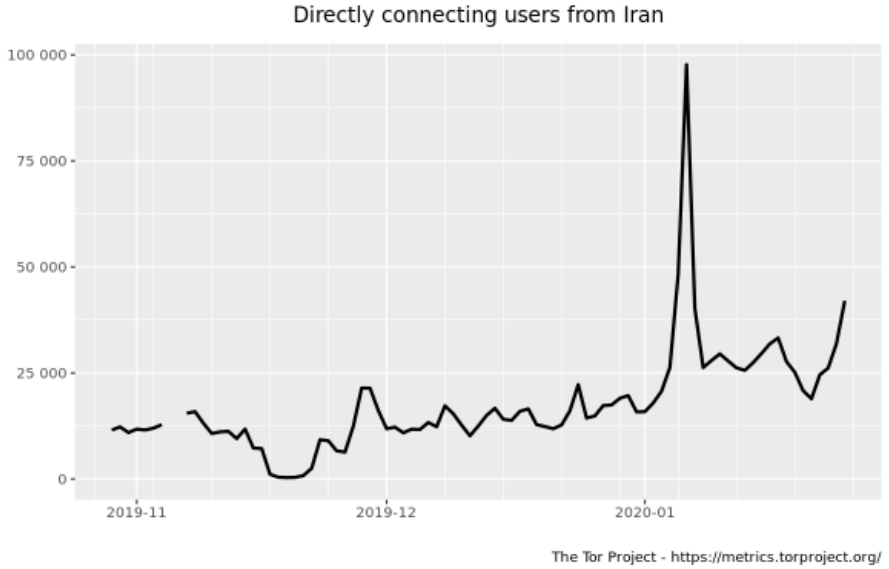
Vorstellung Tor Metrics

Beispiel Iran – Directly connecting users

Relay users | Bridge users by country | Bridge users by transport | Bridge users by country and transport | Bridge users by IP version

BridgeDB requests by requested transport | BridgeDB requests by distributor | Top-10 countries by relay users

Top-10 countries by possible censorship events | Top-10 countries by bridge users | “The anonymous Internet”



Start date: 29.10.2019

End date: 27.01.2020

Source: Iran

Show possible censorship events if available: Off

Update graph

Download graph as PNG or PDF.

Download data as CSV.

Learn more about the CSV data format or how to reproduce the graph data.

This graph shows the estimated number of directly-connecting clients; that is, it excludes clients connecting via bridges. These estimates are derived from the number of directory requests counted on directory authorities and mirrors. Relays resolve client IP addresses to country codes, so that graphs are available for most countries. Furthermore, it is possible to display indications of censorship events as obtained from an anomaly-based censorship-detection system (for more details, see this technical report). For further details see these questions and answers about user statistics.

Sicherheit im Allgemeinen

Kommt auf Nutzung an

Tor Browser – JS, HTML-Media

Whonix, Tails, etc.

Umgebung der Nutzung

Sicherheit im Allgemeinen

onion v2 / onion v3 Services

Onion Services v2, SHA1, DH-Schlüsseltausch und Public Key Kryptografie RSA 1024 Bit. 16 Zeichen lang:

vwakviie2ienjx6t.onion

Onion Services v3 seit Tor Version 3.2, aktuelle kryptografischen Funktionen, SHA3, ECDHE mit ed25519, Public Key elliptische Kurven mit curve25519, 56 Zeichen lang:

4acth47i6kxnvkewtm6q7ib2s3ufpo5sqbsnzjpbi7utijcltosqemad.onion

(Inter)national

Iran (Zensur, Abschaltung, digitaler Widerstand)

China (Great Firewall, meek-x)

EU/BRD (Repression zwiebelfreunde)

Angriffe (FBI/Onionscan, NSA, Great Firewall, Russland)

(Inter)national

An die Verantwortlichen:

Hört auf mit IP Ranges Blocking und dem anderen Zensur Scheiss. Ihr schadet der Gesellschaft und dem Netz. Ihr helft damit nur den Überwachenden.

Fördert den Betrieb und die Nutzung von Tor, Onion Services und dem Ökosystem

Los geht‘s!

Tor nutzen

Tor erklären

Tor verteidigen

Tor machen

(Netz)Politik überprüfen, wählen und machen

Vielen Dank!

Links

Kontakt cryptocation@mailbox.org – bccxmpp@jabber.systemli.org – lugfrankfurt.de Mailingliste

Project

https://www.torproject.org/about/history/
https://community.torproject.org/

Netzwerk/Design

https://metrics.torproject.org/

https://web.archive.org/web/20161019151220/https://people.torproject.org/~isis/slides/2016-10-13-waterloo-handout.pdf

https://riseup.net/de/security/network-security/tor/onionservices-best-practices

Applikationen / OS / Tools

https://tails.boum.org

https://whonix.org

torsocks – Linux Manual https://linux.die.net/man/8/torsocks

https://onionshare.org/ / https://github.com/micahflee/onionshare

Orbot – div. AppStores, Google PlayStore

Briar Messenger – Google PlayStore

Proxy Einstellungen in div. Apllikationen

https://ahmia.fi - http://msydqstlz2kzerdg.onion/

Diverses
https://www.privacy-handbuch.de/handbuch_24f.htm

https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/archiv-datenschutznews/news/brauchen-wir-das-darknet-501090

https://medium.com/beyond-install-tor-signal/case-file-jeremy-hammond-514facc780b8