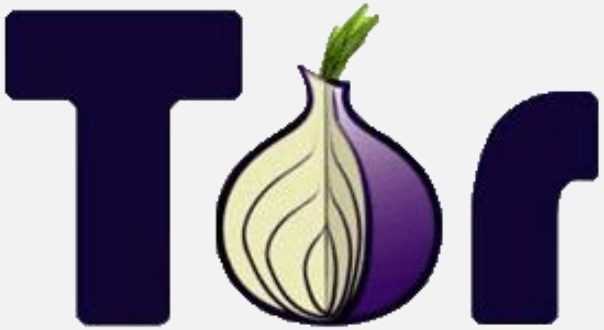


The Second Generation Onion Router

Stefan Hasenauer, Christof Kauba, Stefan Mayer

Übersicht

- Einleitung
- Verfahren zur Anonymisierung
- Allgemeines über Tor
- Funktionsweise von Tor
- Hidden Services
- Mögliche Angriffe

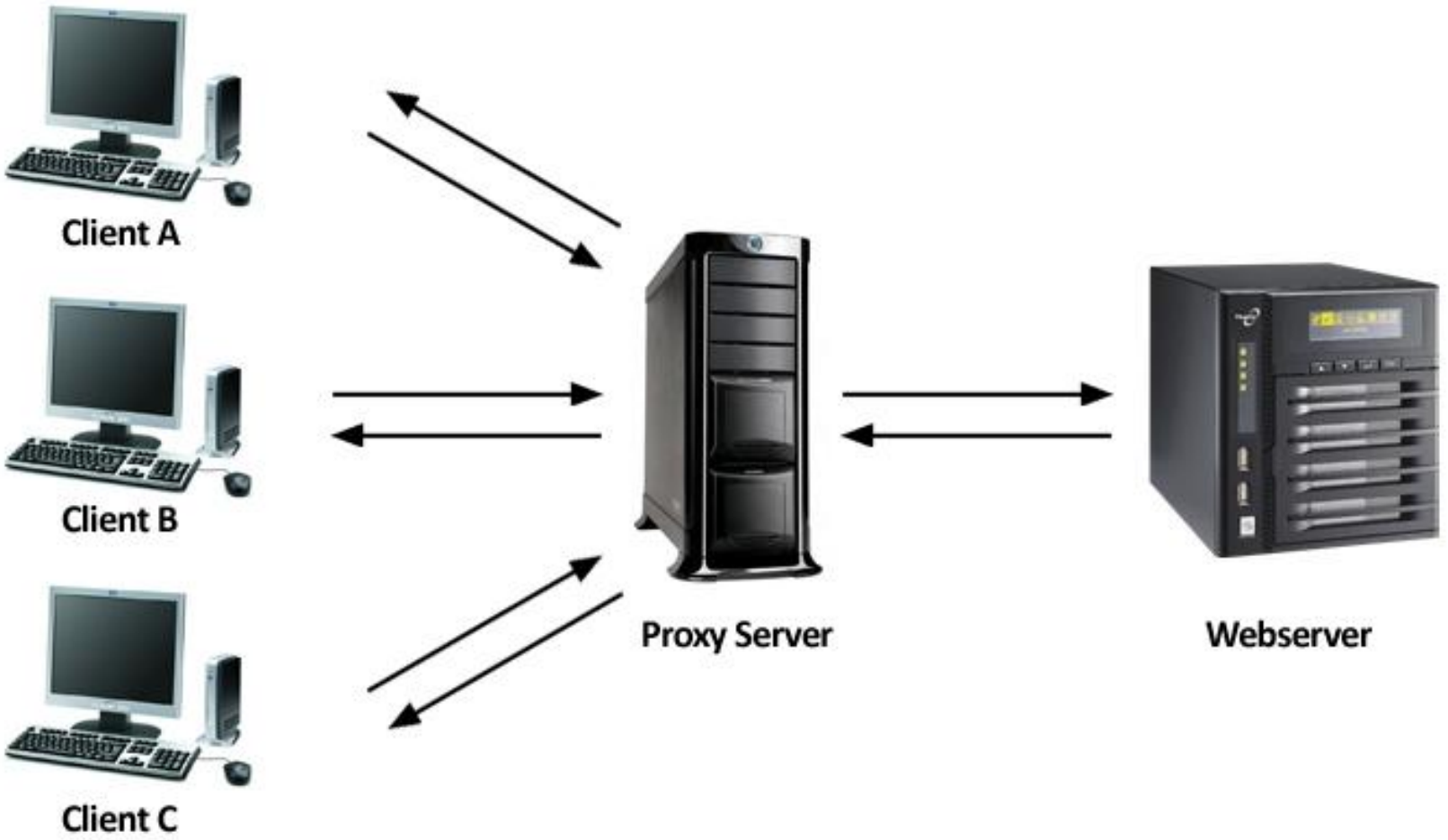
Einleitung

- Identifizierung im Internet
- Zweck der Anonymisierung
  - Schutz vor Traffic Analysis
  - Nutzdaten ev. verschlüsselt, aber IP-Paketheader immer unverschlüsselt
  - Angreifer kann ermitteln wer mit wem kommuniziert
- Verfahren zur Anonymisierung
  - Proxy
  - Mix-Kaskaden
  - Onion Routing

Proxy

- Stellvertreter kümmert sich um Client-Server-Kommunikation
- Webproxy vs. anonymisierender Proxy
- Betreiber eines öffentlichen Proxies kann Daten aufzeichnen bzw. fälschen

Proxy

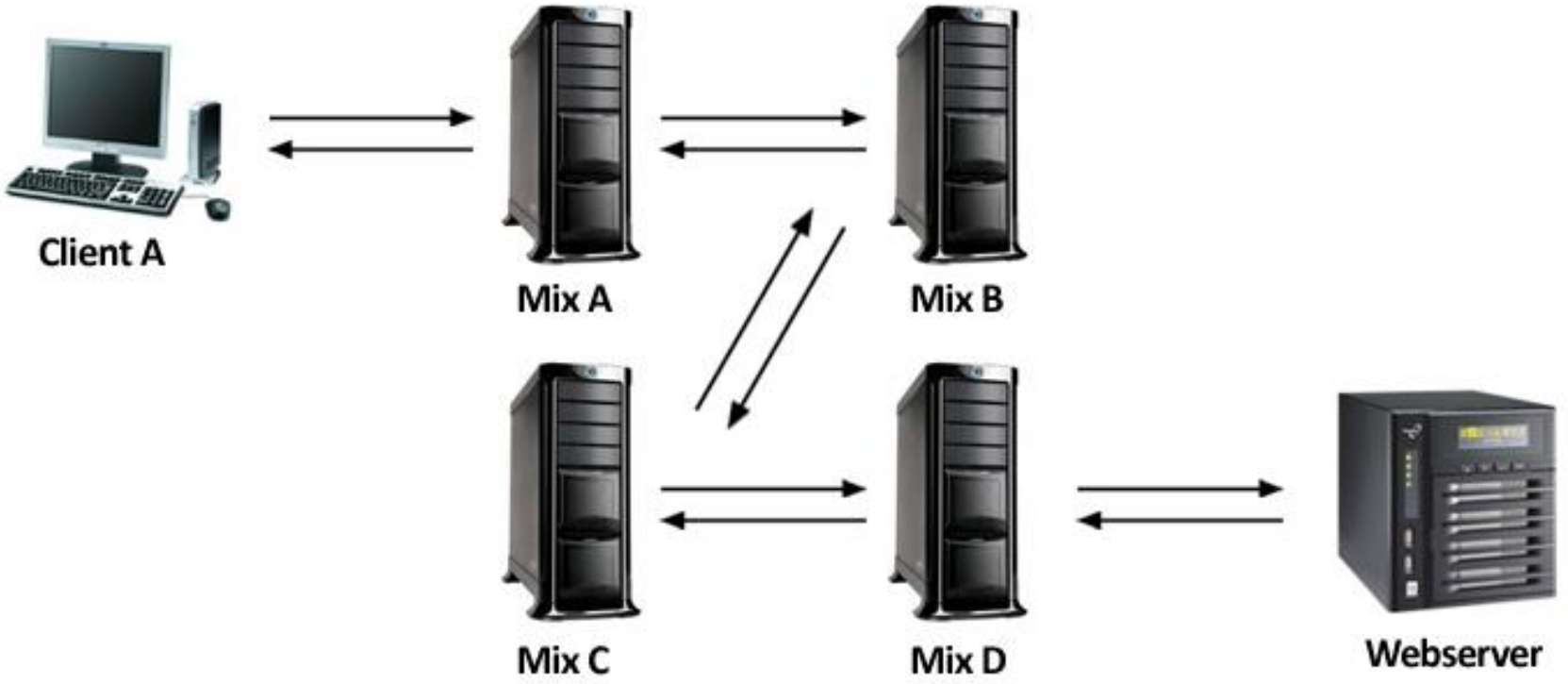


Proxy

- Vorteile:
  - einfache Realisierung
  - schnellerer Zugriff auf immer die gleichen Daten
  - Kosteneinsparung beim Internet-Datenverkehr
- Nachteile:
  - nicht jede Anwendung unterstützt Proxies
  - Sicherheit hängt von Vertrauenswürdigkeit der Server ab

Mix-Kaskaden

- Hintereinanderschaltung von Proxies

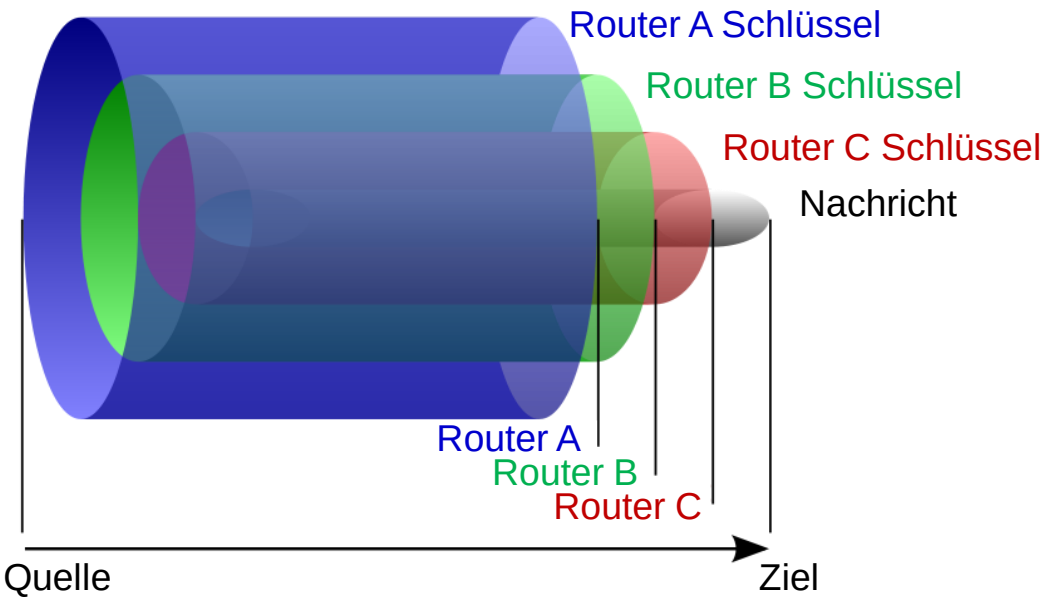


Mix-Kaskaden

- Vorteil
  - Daten werden mehrfach verschlüsselt und über mehrere Rechner geleitet.
- Nachteil:
  - In der Praxis sind sehr viele Abstriche zu machen

Onion Routing

- Webinhalte werden über ständig wechselnde Routen von mehreren Mixen geleitet
- TOR basiert auf dem Onion Routing Konzept mit Erweiterungen



Onion Routing

- Vorteile
  - Lastverteilung
  - Verfolgung sehr schwer
- Nachteile:
  - Keiner möchte Endknoten sein
  - Man-in-the-middle-attack möglich

Eigenschaften von TOR

- Low Latency Anonymous Network
- TCP-Verbindungen
- Mehrere TCP Streams auf einem Circuit
- Perfect Forward Secrecy
- End-to-End Integritätskontrolle
- Hidden Services, Rendezvous Points

Architektur von TOR

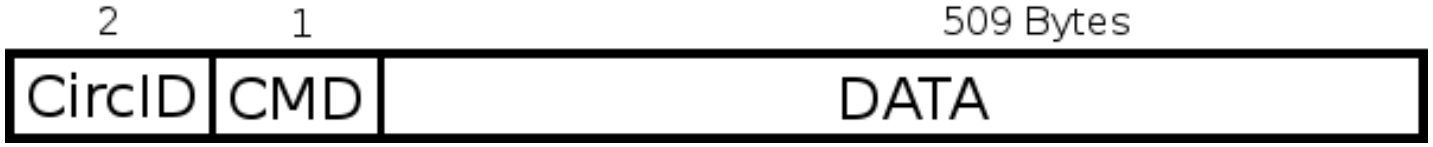
- Onion Proxy
  - Installiert auf lokalem Rechner
- Onion Router
  - Netzwerkknoten für Verbindungen
- Directory Servers
  - Vertrauenswürdige Server mit Liste aktueller Onion Router

TOR Protokoll

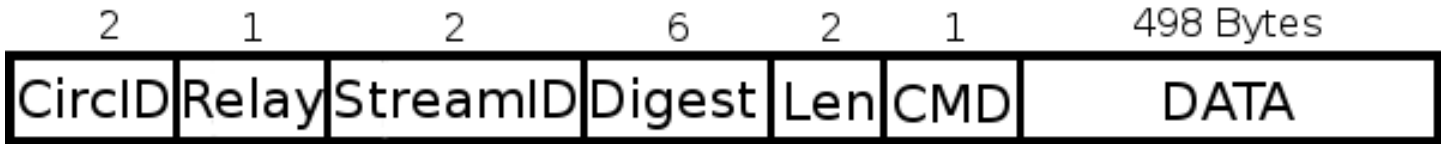
- Verbindungen sind TLS gesichert
- Kurzlebige Schlüssel (symmetrisch, AES)
- Pakete mit fixer Größe von 512 Byte
- End-to-End Integritätsprüfung mittels SHA-1
- Jeder Knoten kennt nur seinen Vorgänger und Nachfolger

Pakete bzw. Zellen

- Control Cells:
  - Aufbau und Steuerung der Verbindung



- Relay Cells:
  - Verbindungsdaten oder Control Cells für nachfolgenden Knoten



Verbindungsaufbau (Circuit)

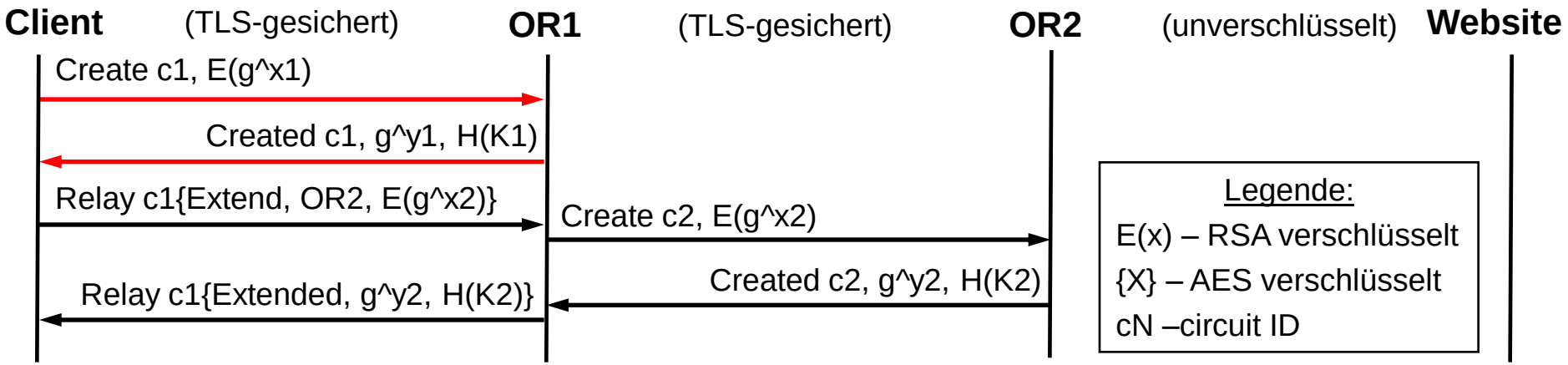
- Onion Proxy holt sich bei einem Directory Server die Liste aktueller Onion Router

Verbindungsaufbau (Circuit)

- Wählt einen zufälligen Einstiegspunkt (Onion Router) aus und baut zu diesem eine TLS gesicherte Verbindung auf

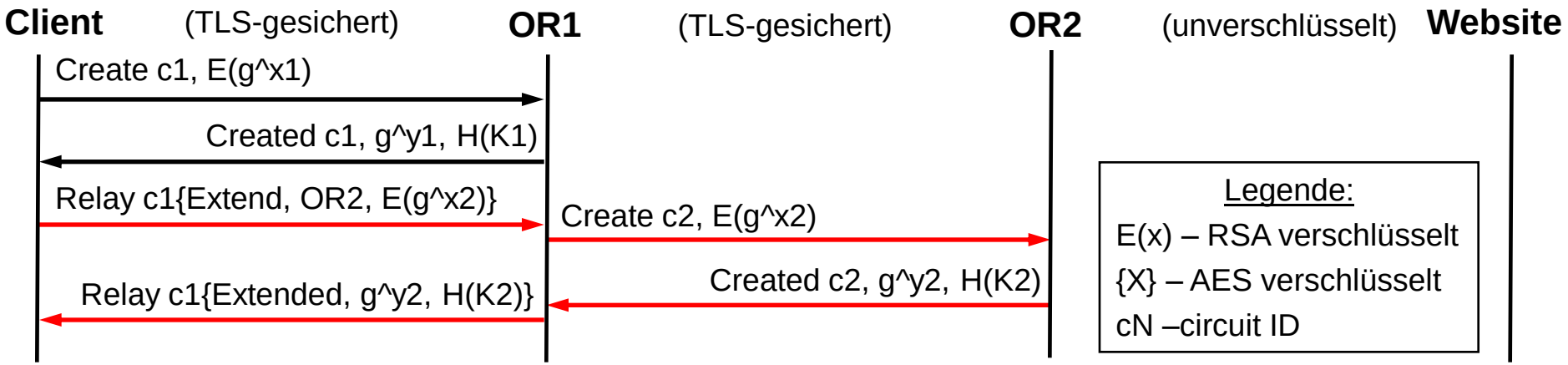
- Onion Proxy kennt die öffentlichen RSA Schlüssel (Onion Key) der Onion Router für sicheren Schlüsselaustausch

Verbindungsaufbau im Detail



- OP vereinbart einen symmetrischen Schlüssel für die Verbindung zum ersten Onion Router nach dem Diffie-Hellman Verfahren
- Create Control Cell

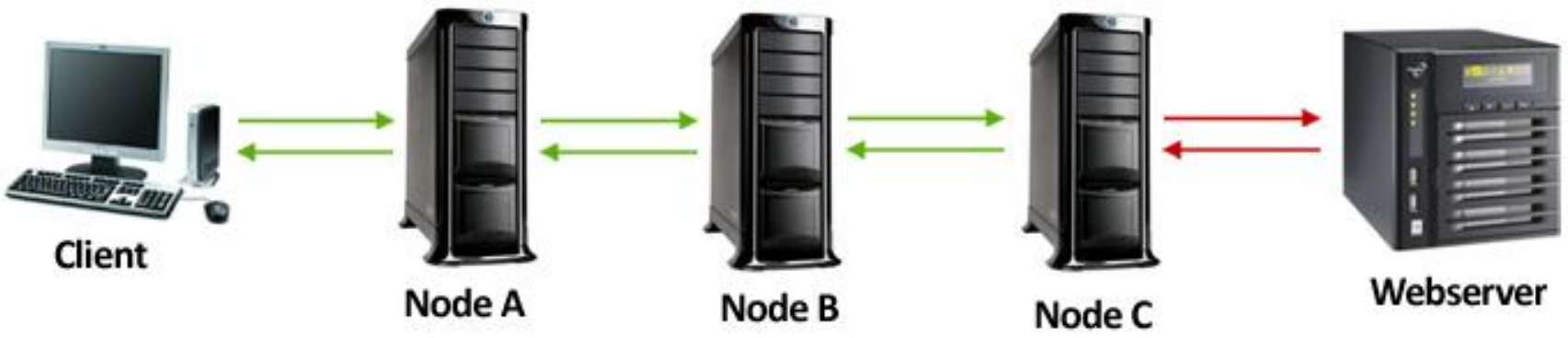
Verbindungsaufbau im Detail



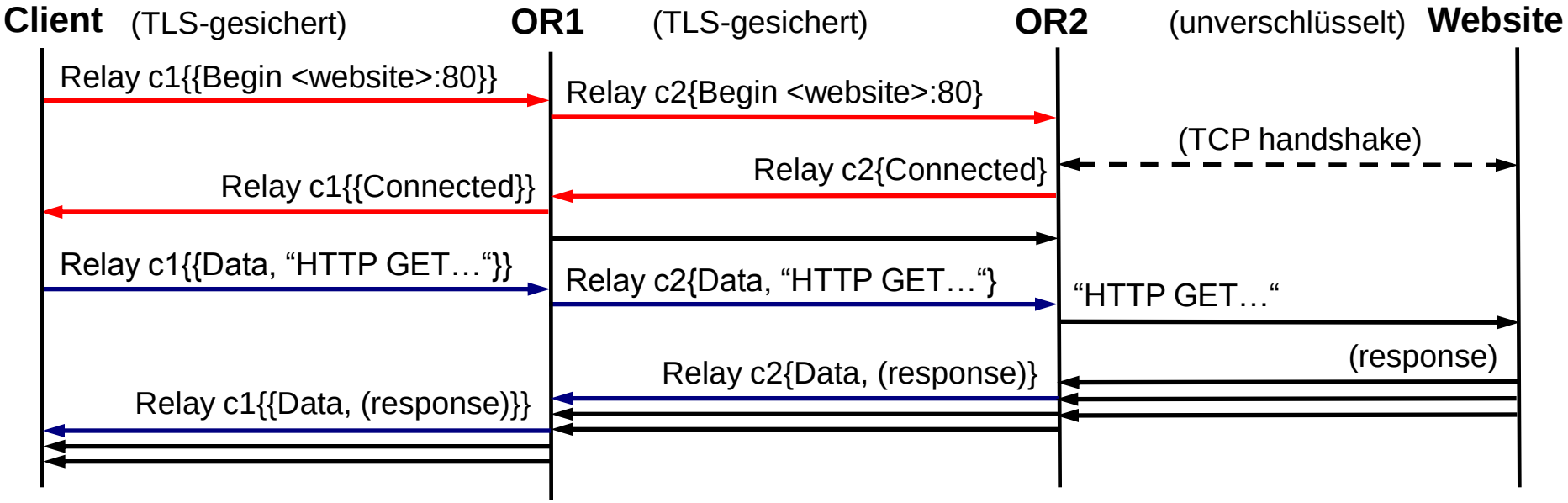
- Verbindung wird noch einen Onion Router erweitert, mit diesem wird wieder ein neuer Schlüssel vereinbart
- Extend Relay Cell, Create Control Cell

Eigenschaften eines Circuits

- Jeder Circuit nur ca. 10 min aktiv
- Daten vom letzten Knoten zum Empfänger werden unverschlüsselt übertragen
- TCP basierte Kommunikation kann über den Circuit getunnelt werden



Datenübertragung



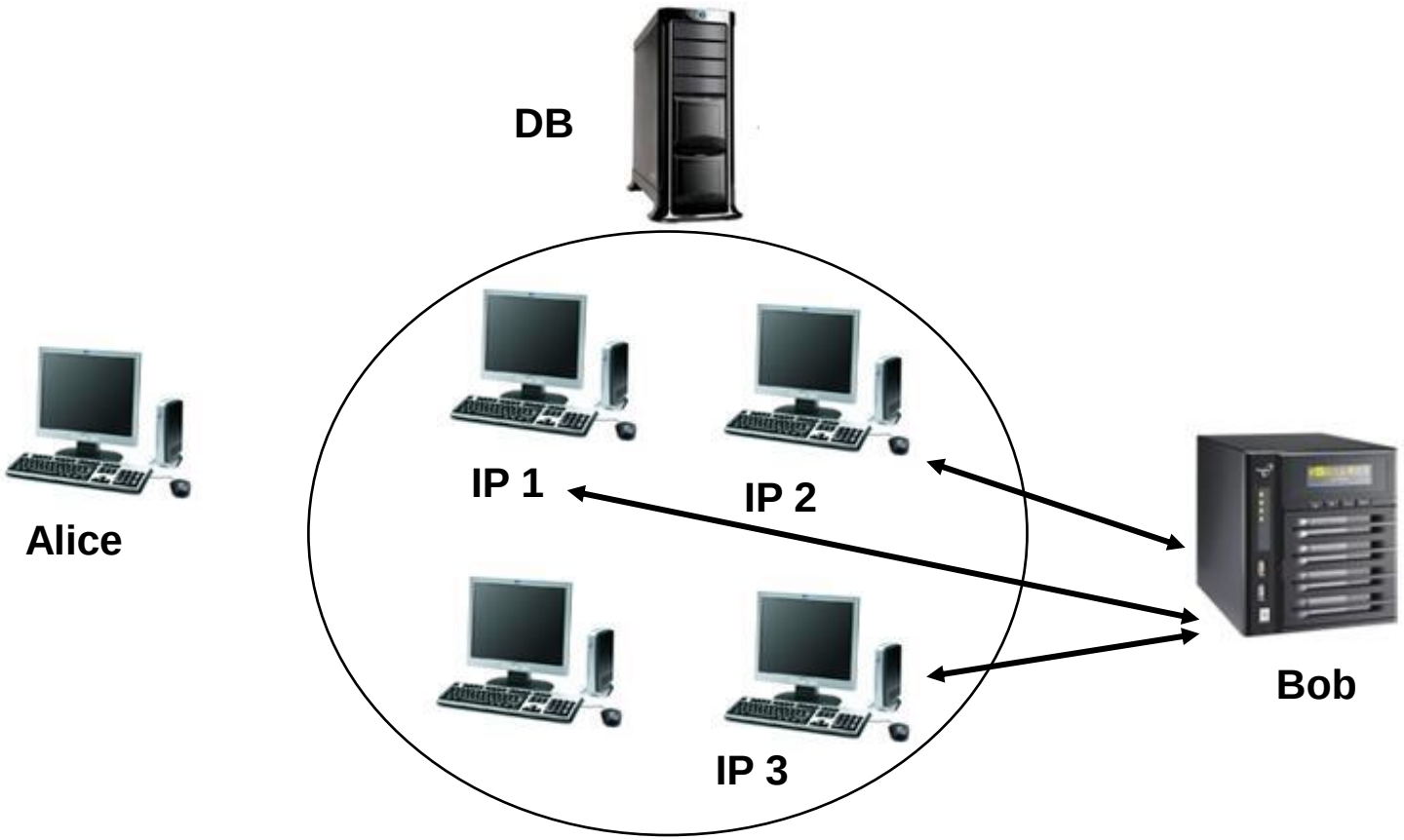
- Öffnen eines/mehrerer Streams
- Relay Cells: Begin, Connected, Data und End
- Schrittweises Ent-/Verschlüsseln entlang des Circuits

Location Hidden Services

- Location-Hidden Services
- Anbieten von TCP-Diensten
- IP-Adresse (des Servers) bleibt geheim
- Ziele:
  - Zugangskontrolle
  - Robustheit
  - Smear-Resistance
  - Applikationstransparenz
- Journalisten, Dissidenten, Unternehmen, Regierungen

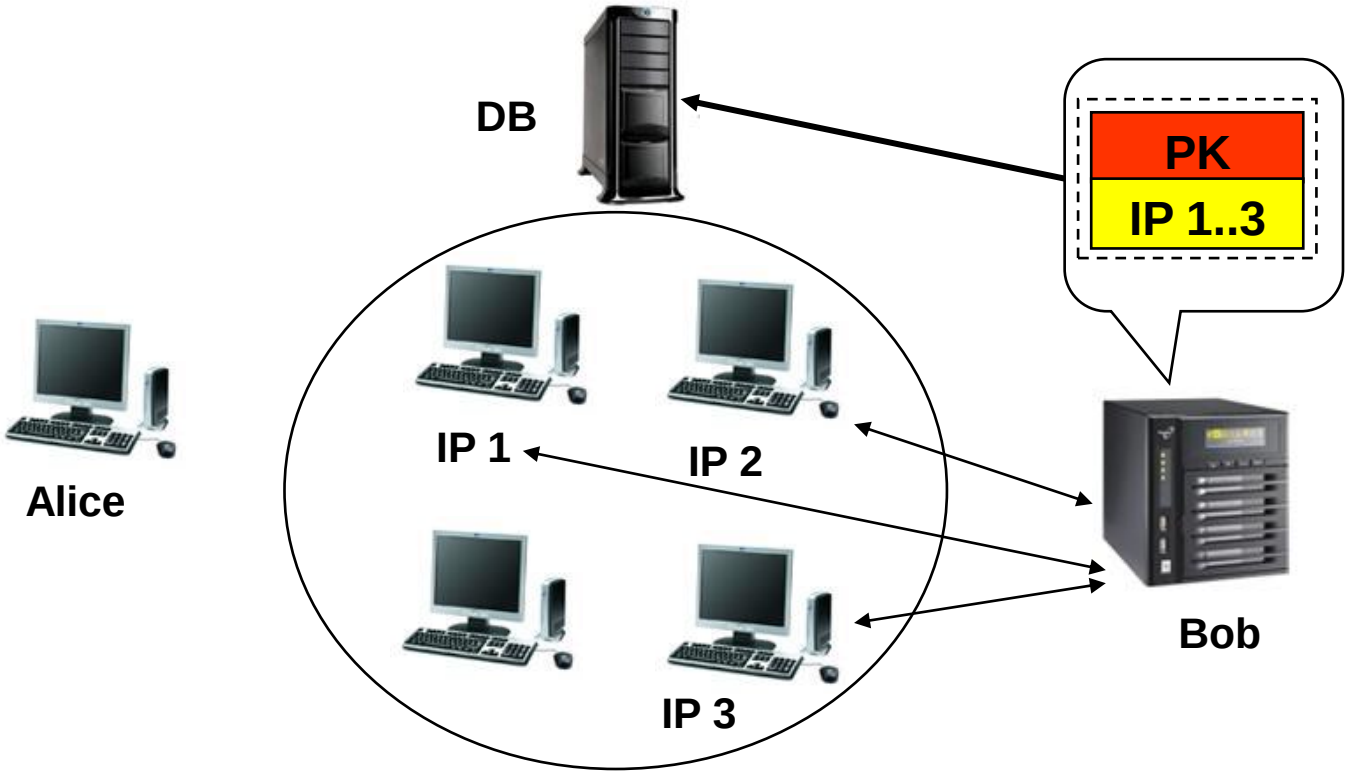
Location Hidden Services

1. Bob wählt Introduction Points (IP) aus



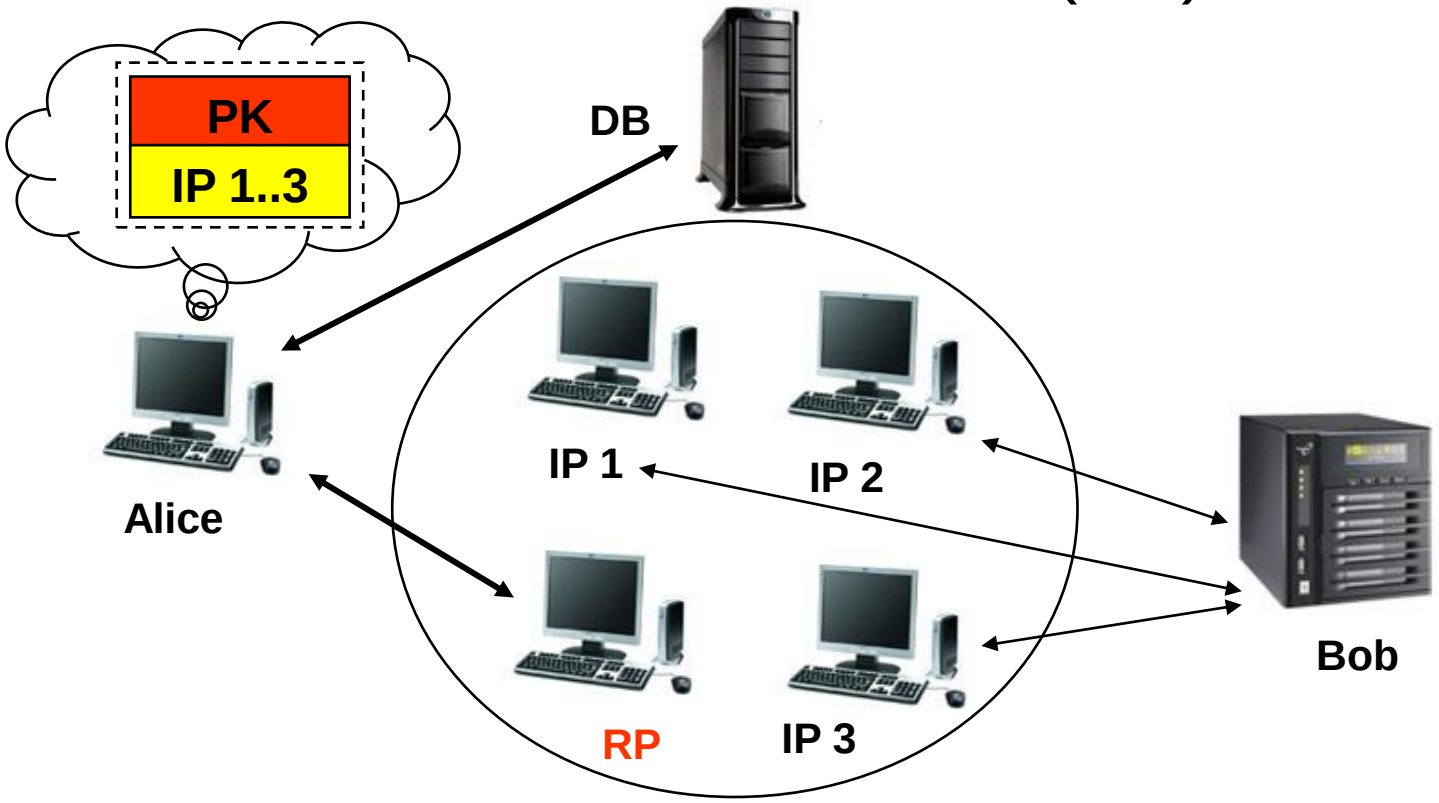
Location Hidden Services

2. Erstellung Services Descriptor
3. Hinterlegung in Datenbank



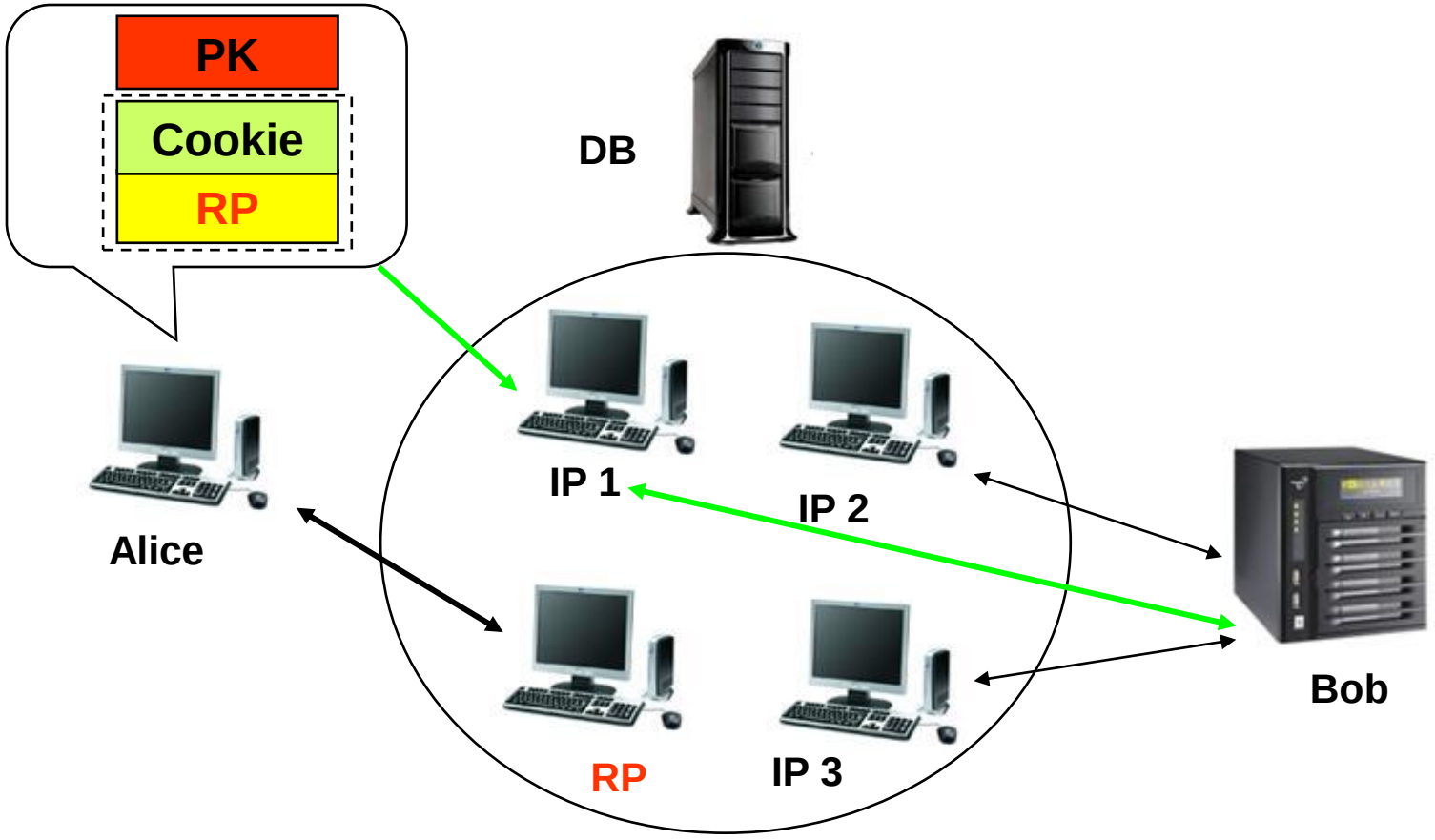
Location Hidden Services

4. Alice will Dienst verwenden, befragt Datenbank
5. Alice erstellt Rendezvous Point (RP)



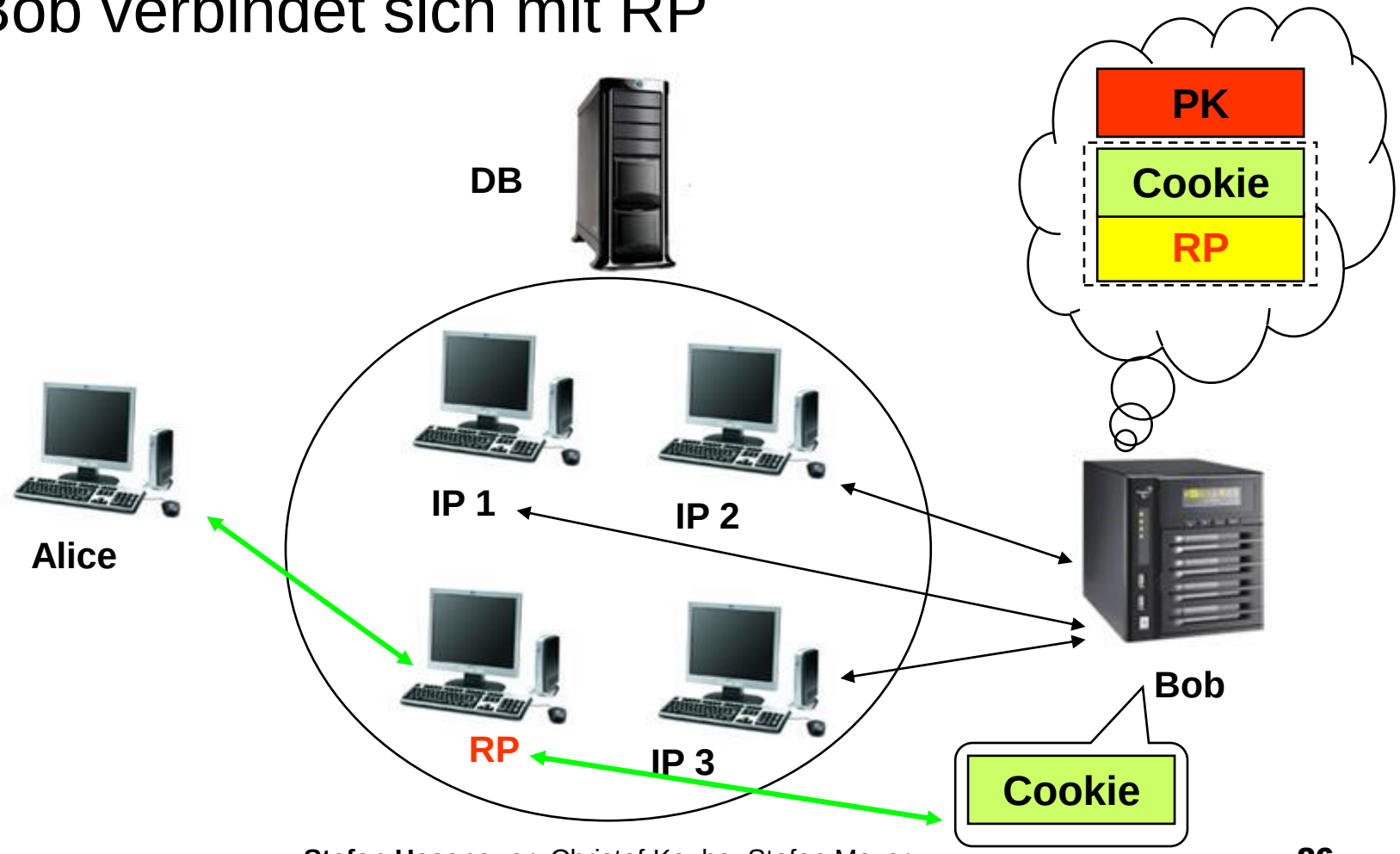
Location Hidden Services

6. Alice sendet Nachricht an Bob



Location Hidden Services

7. Bob verbindet sich mit RP



Mögliche Angriffe

- Passive Attacken
  - Auslesen der Userdaten
    - Gegenmaßnahmen: Privoxy, Verschlüsselung SSL/TLS
  - Verkehrsflussanalyse
    - Gegenmaßnahme: Verbindung zw. Onion Proxy und Onion Router verstecken
  - Website Fingerprinting
    - Verkehrsmuster bestimmter Webseiten wiedererkennen

Mögliche Angriffe

- Aktive Attacken
  - Kompromittierter Onion Proxy
    - Gegenmaßnahme: Hashwerte für Versionen
  - DoS-Attacke gegen unbeobachtete Onion Router
  - Bösartiger Onion Router
    - Muss erster und letzter Knoten im Circuit sein

Mögliche Angriffe

- Attacken gegen Verzeichnisserver
  - Verzeichnisserver zerstören
  - Verzeichnisserver übernehmen
- Attacken gegen Rendezvous Points
  - Introduction Point attackieren
  - IP oder RP kompromittieren

Vielen Dank für Ihre Aufmerksamkeit!