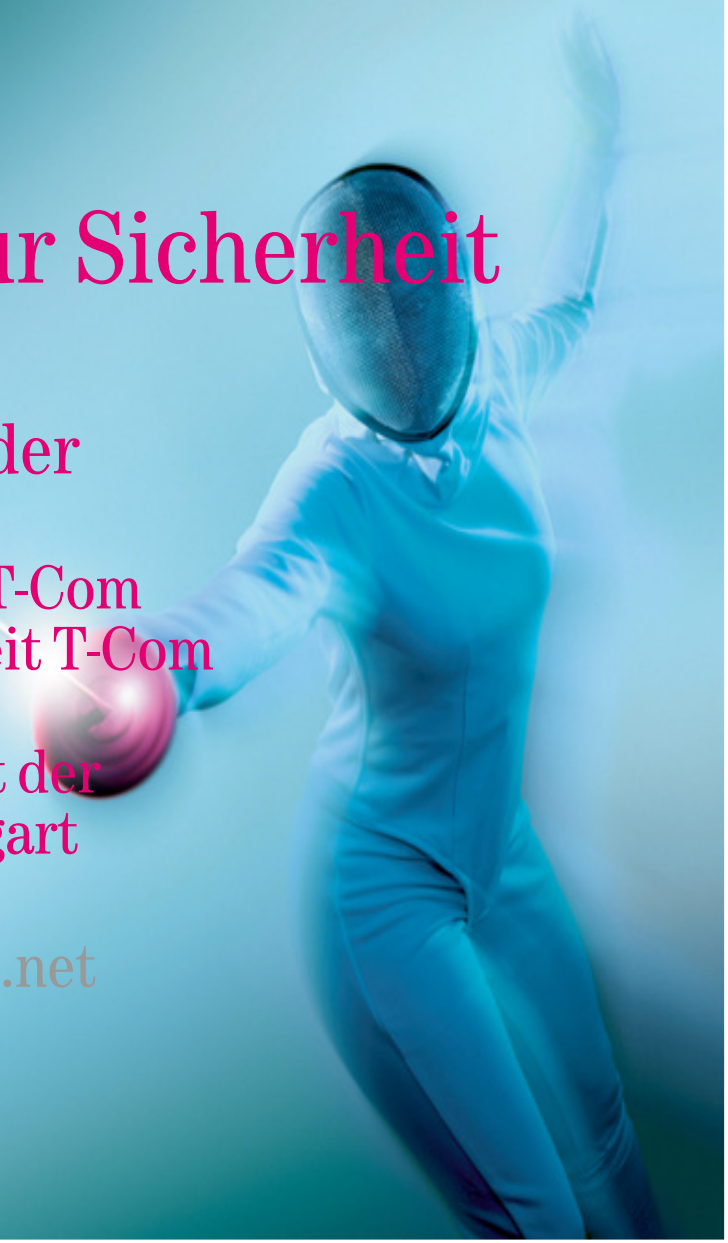
ENUM und Fragen zur Sicherheit

Gerhard Schröder

Deutsche Telekom, T-Com
Unternehmenssicherheit T-Com

in Kooperation mit der
Universität Stuttgart

schroederg@t-com.net

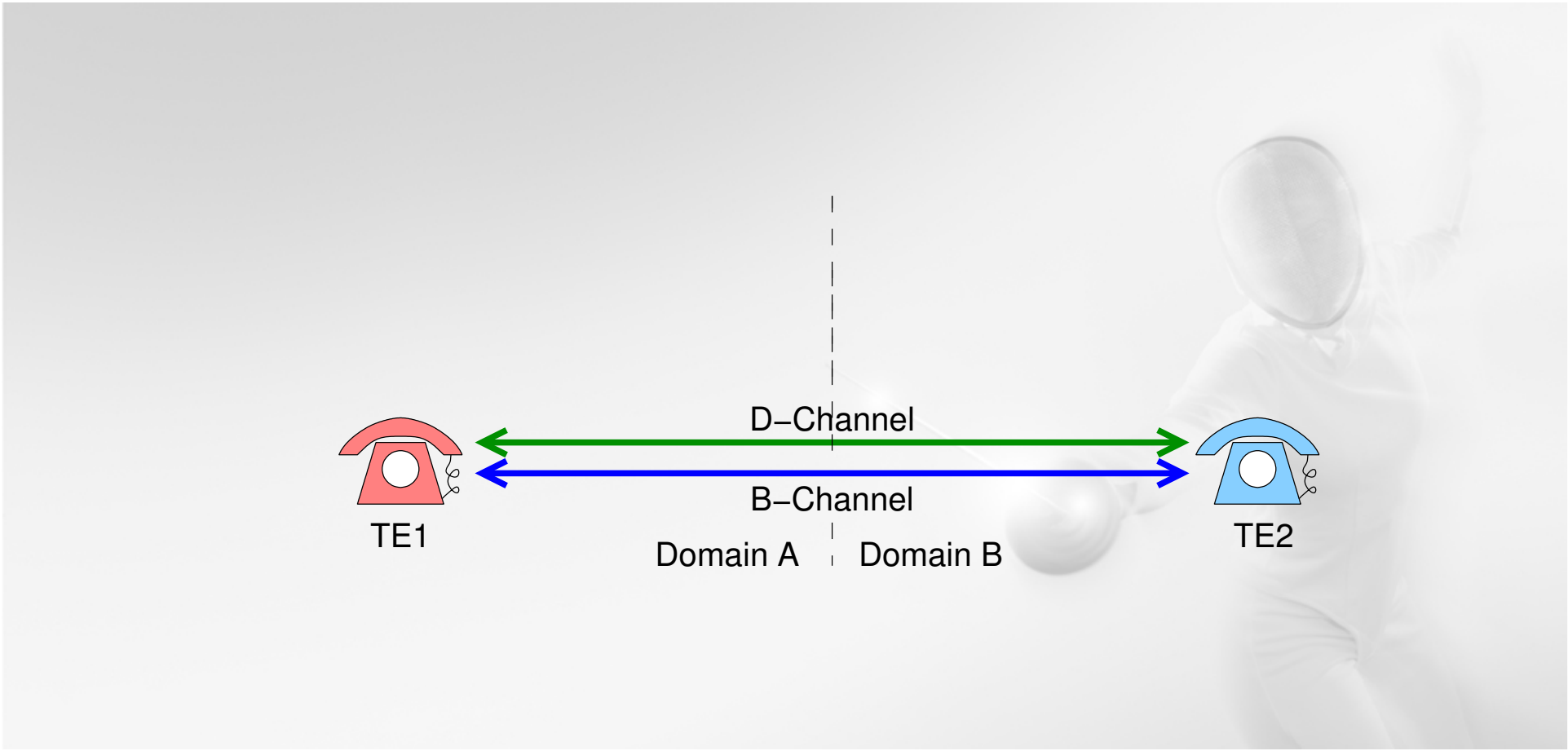


Untersuchungen zur Sicherheit von ENUM

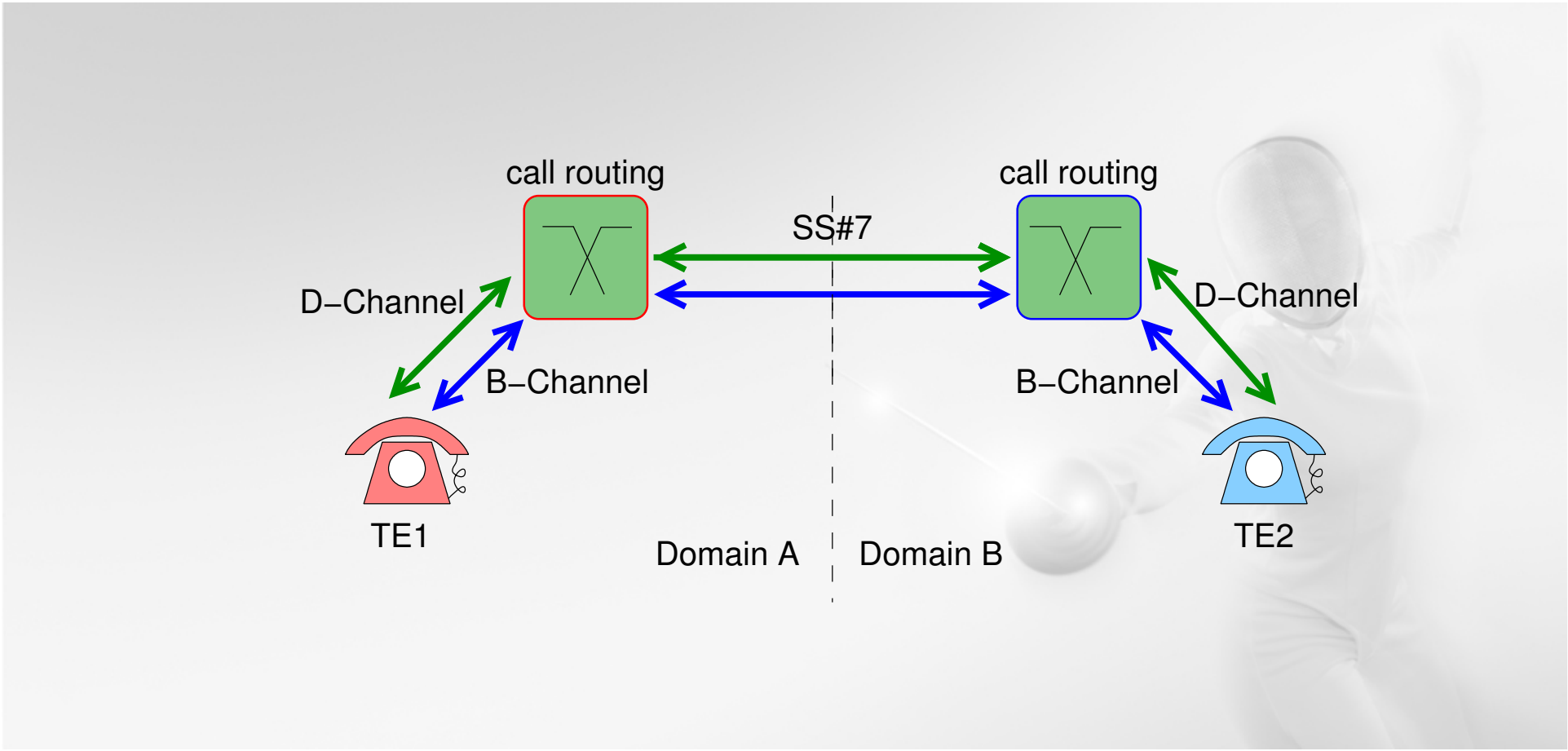
- **Grundlagen**
- **ENUM im offenen Internet**
  Sicherheit der DNS-Infrastruktur
  DNSSEC
- **Komplexe Umsetzungen mit nicht-terminalen Records**
  Regular Expressions
  DDDS
  Routing zwischen Vertrauensdomänen
  Routing zwischen offenen und geschlossenen SIP-Plattformen
- **Probleme der Spezifikation und Implementierbarkeit von ENUM/DDDS**
- **Zusammenfassung und Empfehlungen**

T-Com

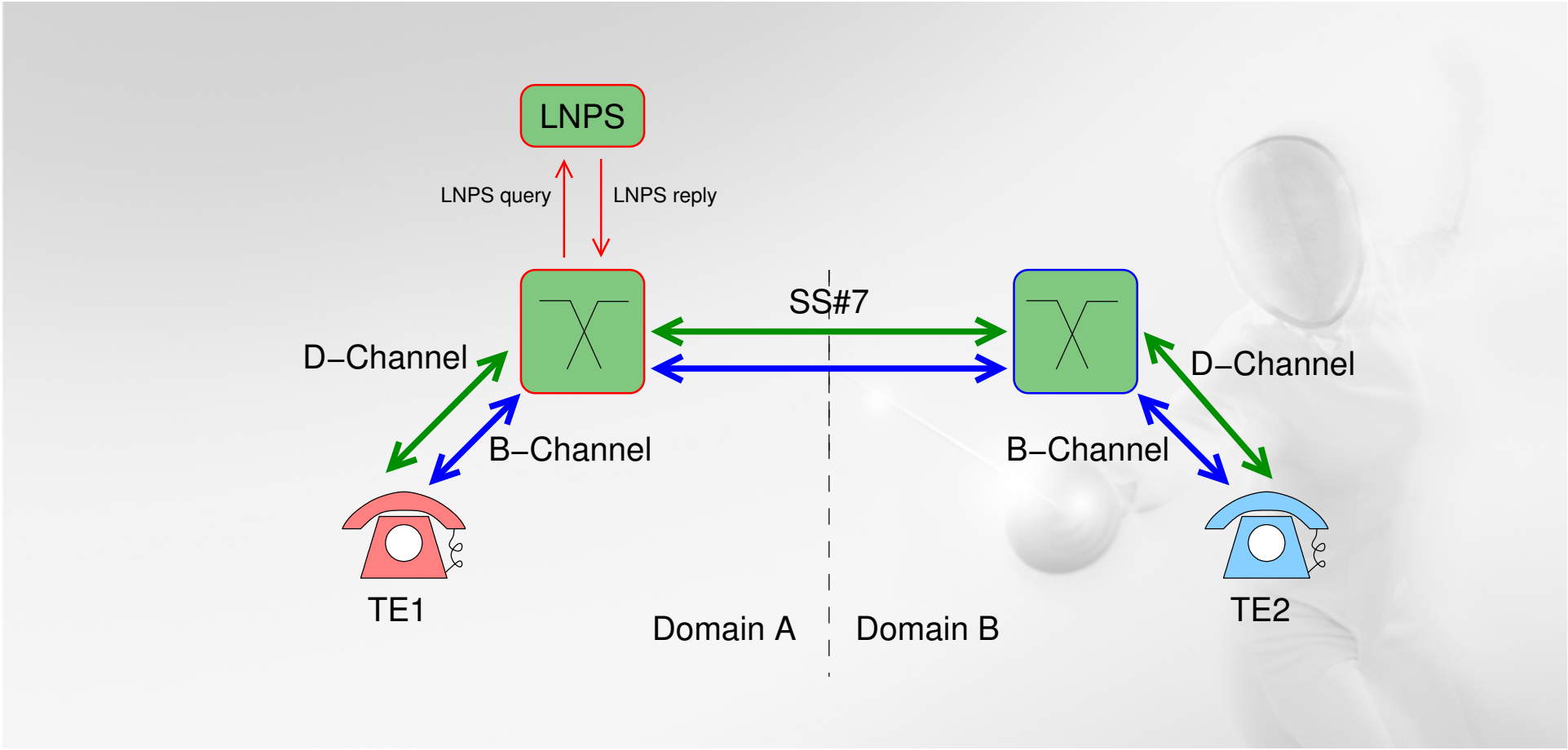
ISDN Verbindung (I)



ISDN Verbindung (II)



ISDN Verbindung (III)



ISDN

Szenario: ISDN-Telephonie:

- Adressierung durch Nummern entsprechend E.164
- Jede MSN (Multiple Subscriber Number) ist in der Vermittlungsstelle konfiguriert und einem festen Anschluss zugeordnet.
- Durch entsprechende Signalisierung kann über D-Kanal-Parameter festgestellt werden, ob die Calling Party Number
  a) *network provided*
  b) *user provided and verified*
  c) *default*
  ist
- Damit ist ein sehr leistungsfähiger Mechanismus zur Verifikation bzw. Authentisierung der Rufnummer auf der Empfängerseite vorhanden.

ENUM und SIP

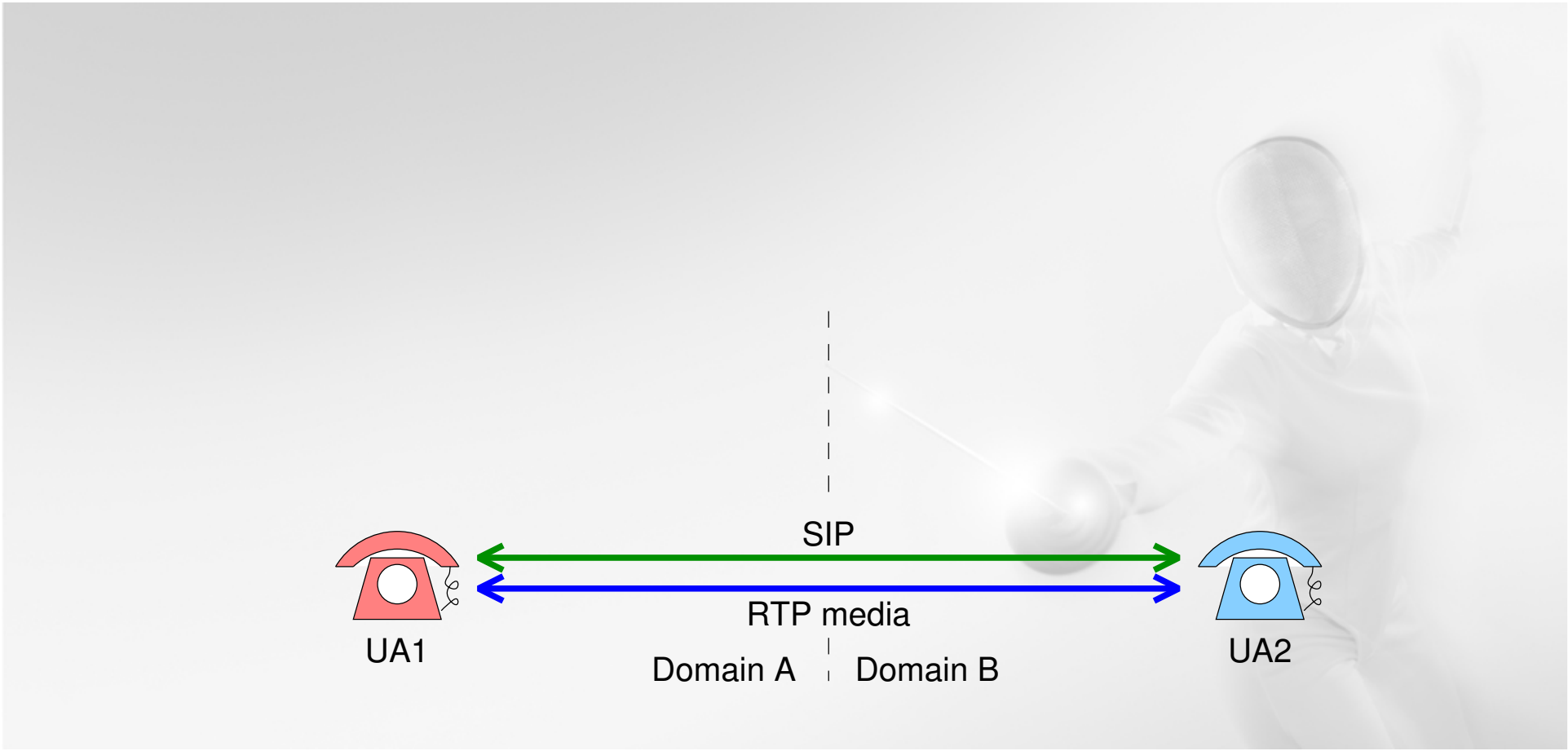
Szenario: IP-Telefonie mit SIP

Möglichkeiten zur Adressierung von Teilnehmern:

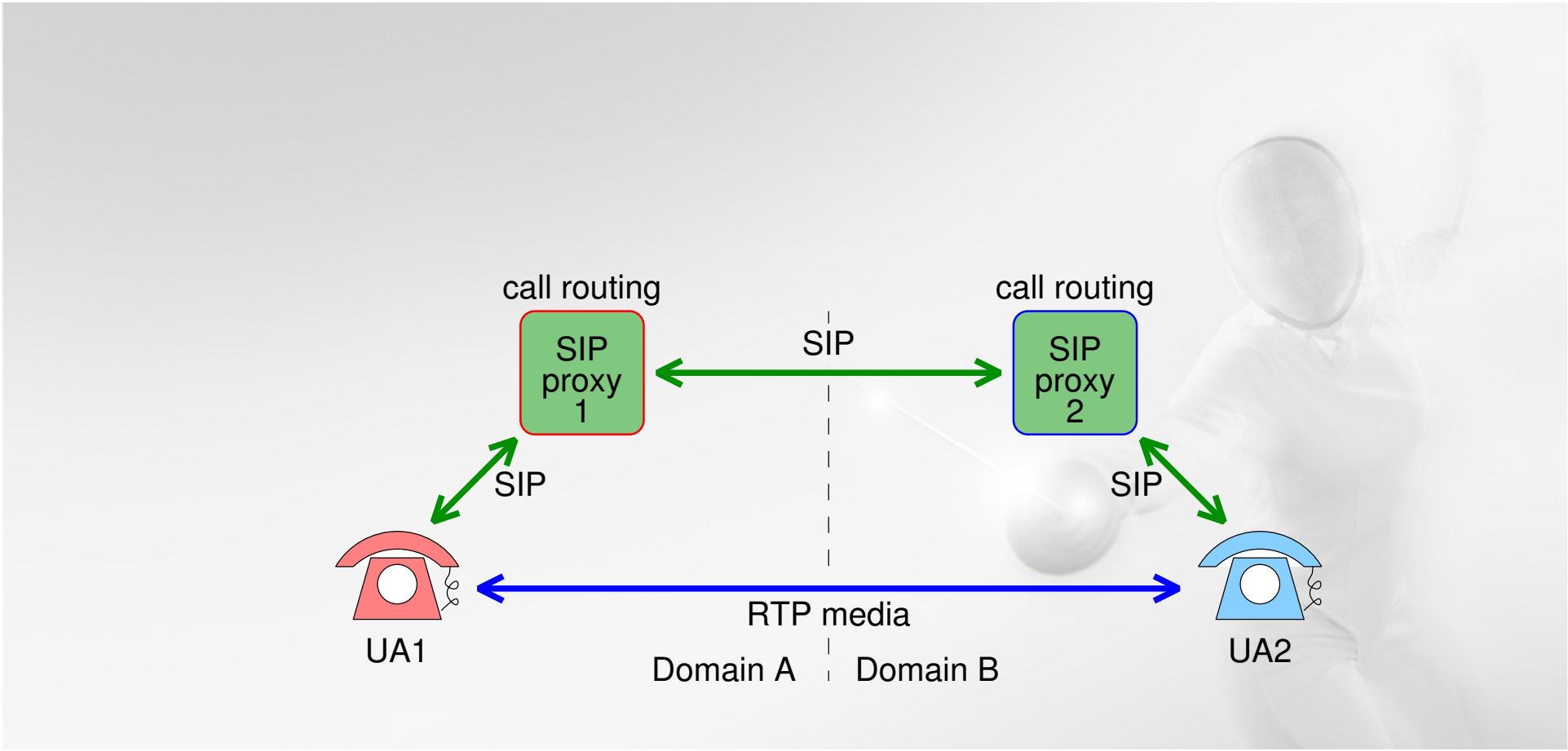
- SIP URI / SIPS URI (Secure SIP = SIP over TLS)
  localpart@domain, z.B. To: Alice <sip:alice@atlanta.example.com>
  auch Angeben von Telefonnummern möglich,
  Interpretation entsprechend lokaler Richtlinie der Domain, z.B.
  To: Paul <sip:+4961514711@sip-to-isdn-gateway.net>
- TEL URI (Erweiterung nach RFC 2806)
  Internationale Telefonnummer nach Standard E.164,
  To: Paul <tel:+49-6151-4711>
- Wünschenswert, um bekannte Nummern weiterverwenden zu können
  Notwendig bei Interconnection mit ISDN (TE kann nur Ziffern wählen)
- SIP Implementierungen müssen (nur) SIP und SIPS unterstützen.
- Proxies dürfen andere Schemata nach SIP/SIPS umsetzen

Ziel ENUM: Umsetzung E.164 → SIP URI (und andere) mit Hilfe des DNS

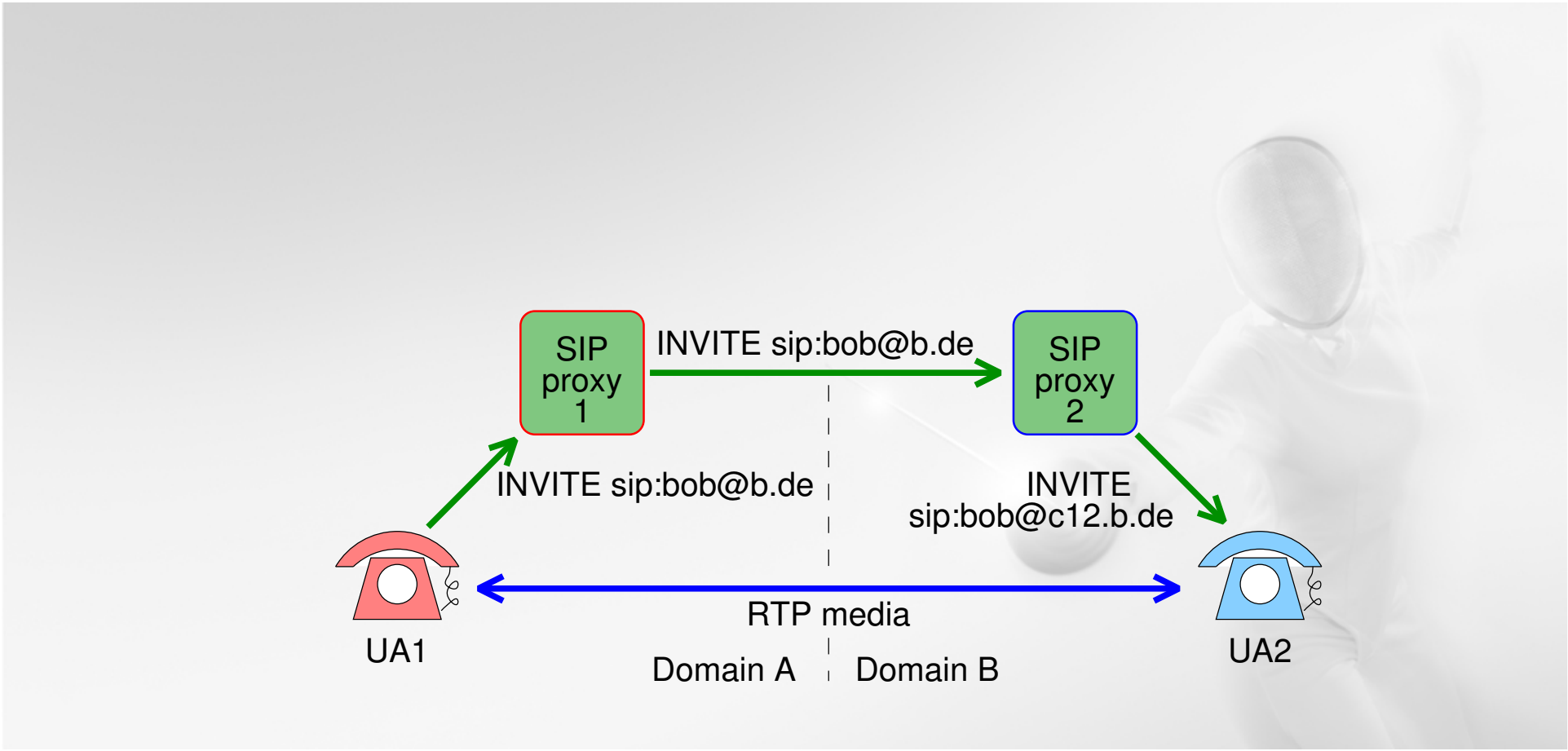
ENUM und SIP (I)



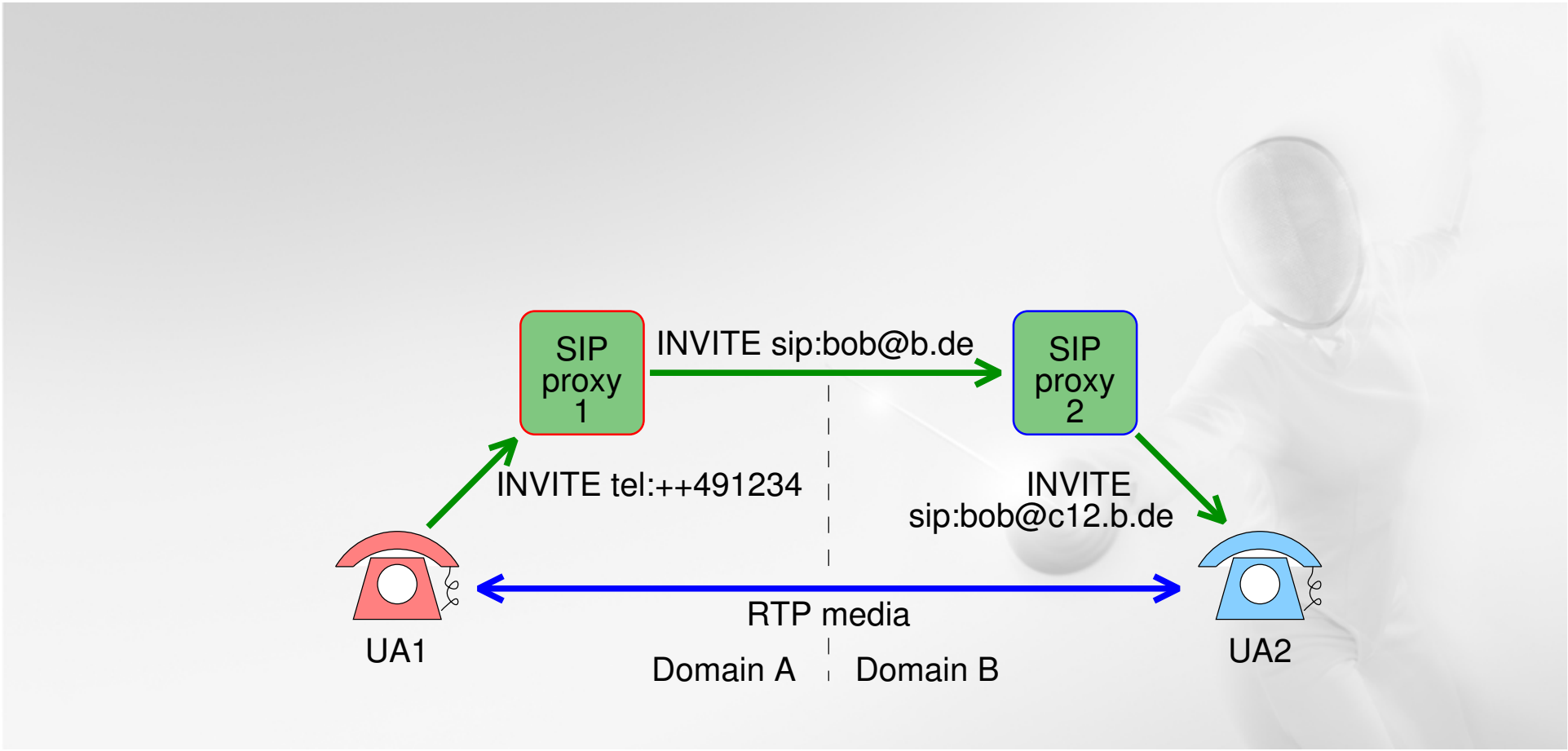
ENUM und SIP (II)



ENUM und SIP (III)

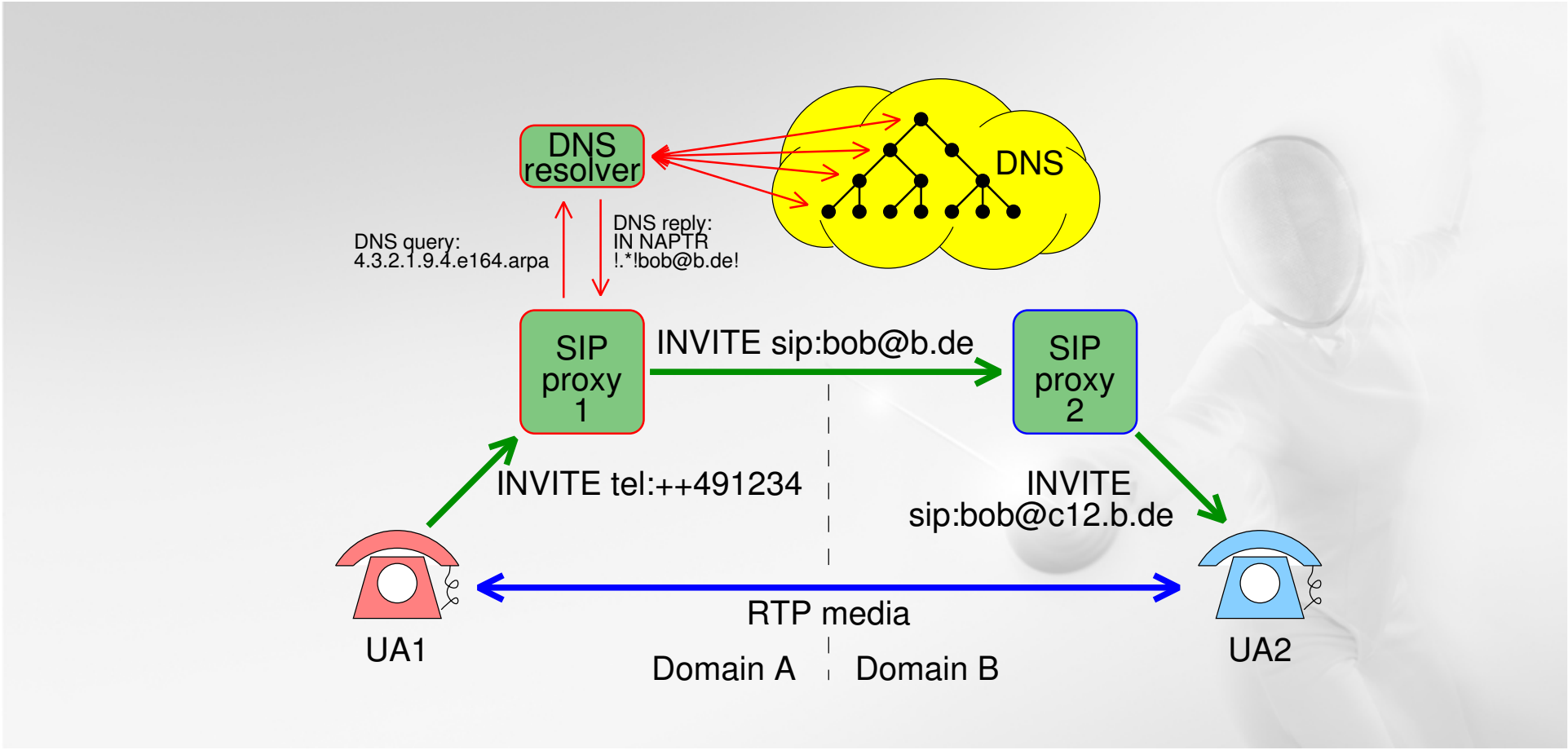


ENUM und SIP (IV)



ENUM und SIP (V)

Ziel ENUM:
Umsetzung E.164 → SIP URI (und andere) mit Hilfe des DNS



ENUM Standardisierung

Ziel ENUM: Umsetzung E.164 → SIP URI (und andere) mit Hilfe des DNS

- RFC 2916 (09/2000): E.164 number and DNS
  Erster RFC zu ENUM
  20 Seiten
  Eintragen und Suchen von E.164-Nummern im DNS, NAPTR record
  Ersetzt durch RFC 3761
- RFC 3401 - 3406 (10/2002): Dynamic Delegation Discovery System
  Verallgemeinertes Konzept für allgemeine Adressabbildungen
  DNS nur eine von vielen (theoretisch denkbaren) Datenbanken
  Noch nicht alle Konzepte vollständig ausgereift
- RFC 3761 (04/2004): ENUM als eine Anwendung des DDDS
  Zusammen mit DDDS Spezifikation: 105 Seiten

ENUM Szenarien

- **Betrachtung der Abbildung auf DNS-Serverstrukturen bei „offenen" Szenarien**
  Abhängigkeiten von externen (Nameserver-)Betreibern
  Untersuchung alternativer Netzkonfigurationen: „geschlossene" SIP Plattformen
  Vom öffentlichen Internet-DNS separates, privates „Infrastructure ENUM"
  Szenarien für Interdomain-Routing
  Einsatz nicht-terminaler Regeln
- **Zusammenschalten offener und geschlossener Plattformen**
  Misch-Szenarien aus Infrastructure ENUM (für netzinterne Rufe) und User ENUM (Rufe von/zu fremden Netzen)
  Sicherstellen zumindest "netzinterner" Rufe

ENUM-Konfiguration „offenes Netz”

- RFC 3761
  ENUM-Einträge für öffentliche E.164-Nummern unterhalb DNS-Wurzel „e164.arpa.”, im öffentlichen Internet-DNS sichtbar
  ENUM/DDDS-Mechanismen dürfen auch unterhalb anderer Wurzeln verwendet werden, dies darf aber nicht ENUM genannt werden
- DENIC eG
  ENUM-Trial bis Dezember 2005,
  9.4.e164.arpa. (derzeit) delegiert an DENIC
  Direktes Registrieren einzelner Rufnummern von Endkunden,
  analog zur Registrierung von .de-Domains (ggf. über Registrare)
  NAPTR-Datensätze im Internet weltweit sichtbar
  → Ansatz “offenes Internet”
  E.164-Nummernvergabe entkoppelt von Netzzugang / Transportdienstleistung
  DNS-Infrastruktur hilft beim Finden des B-TIn, alles Andere: Ende-zu-Ende
  → Probleme: Datenschutz, DoS-Angriffe, VoIP-Spam, ...

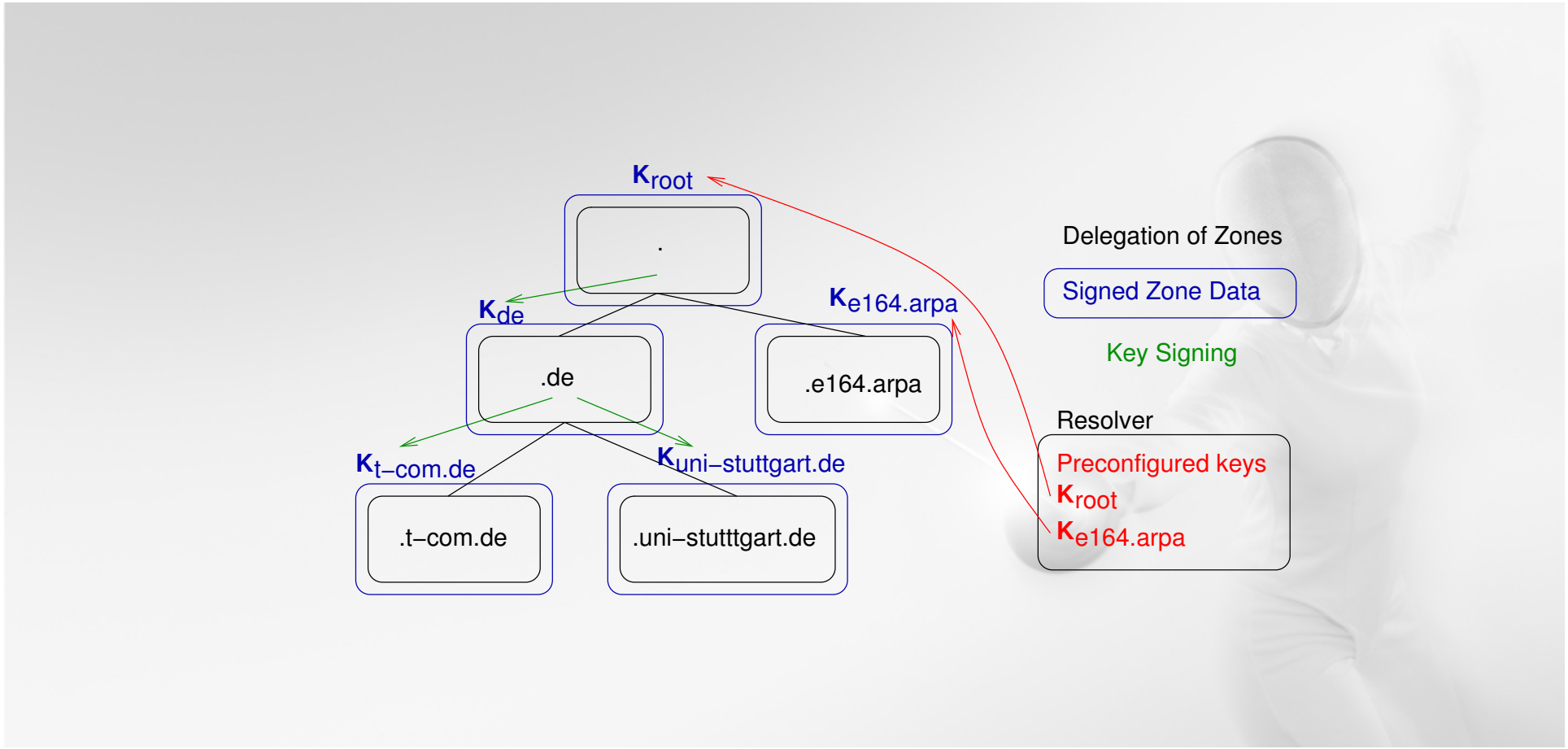
Untersuchungen zur DNS-Serverstruktur

Probleme der DNS-Serverstruktur

- **Integrität von Anfragen**
  Ein kompromierter/fehlkonfigurierter Server im Baum
  → Falsche Antwort auf DNS-Anfrage
  Ausnutzen von Schwachstellen in Implementierungen und im LAN
  DNS Cache Poisoning
  DNS Spoofing

- **Lösungsansatz: DNSSEC**
  DNS Security Extensions RFC4033-4035 (März 2005)
  Schutz der Integrität von DNS-Einträgen durch digitale Signaturen
  Vorkonfigurierte public keys in Resolvern (Trust Anchor)

DNSSEC



DNSSEC

Fragen zu DNSSEC

- **Administrative Probleme einer globalen PKI**
  Verteilung neuer (Root-) Schlüssel
  → Wie werden vorkonfigurierte Schlüssel der Resolver ersetzt?
  Signatur von Schlüsseln für jede neue delegierte Zone nötig
  Änderung von Schlüsseln bedeutet Änderungen in übergeordneter Zone
- **Einige Schwachstellen weiterhin vorhanden**
  Empfindlichkeit für DoS Angriffe
  Implementierungsschwachstellen
- **Schutz der Vertraulichkeit von Einträgen nicht möglich**
  Da auf etabliertem DNS basierend
  Wäre insbesondere für ENUM wichtig

DDDS Regular Expressions

Einfache Umsetzung

```
4.1.1.1.9.4.e164.arpa. IN NAPTR 100 30 "u" "E2U+sip"
"!^.*$!sip:user@carrier.de!„
```

```
+491114      liefert sip:user@carrier.de
```

→ Möglichkeiten der Regular Expression nicht genutzt

Umsetzung von Rufnummernblöcken

```
*.2.1.9.4.e164.arpa. IN NAPTR 100 30 "u" "E2U+sip"
"!\+49123(\d)(\d*)^$!sip:\2@sip-proxy\1.de!„
```

```
+4912345           liefert 5@sip-proxy4.de
+49123556677       liefert 56677@sip-proxy5.de
```

“Geschlossene” SIP-Plattformen

Untersuchung alternativer Netzkonfigurationen

- **„geschlossene” SIP Plattformen**
  z.B. ETSI TISPAN, 3GPP IMS
  Keine bzw. eingeschränkte Ende-zu-Ende IP Konnektivität
  Session Border Controller (Firewalls)
  → Application Layer - Routing-Mechanismen (ggf. Interdomain) benötigt

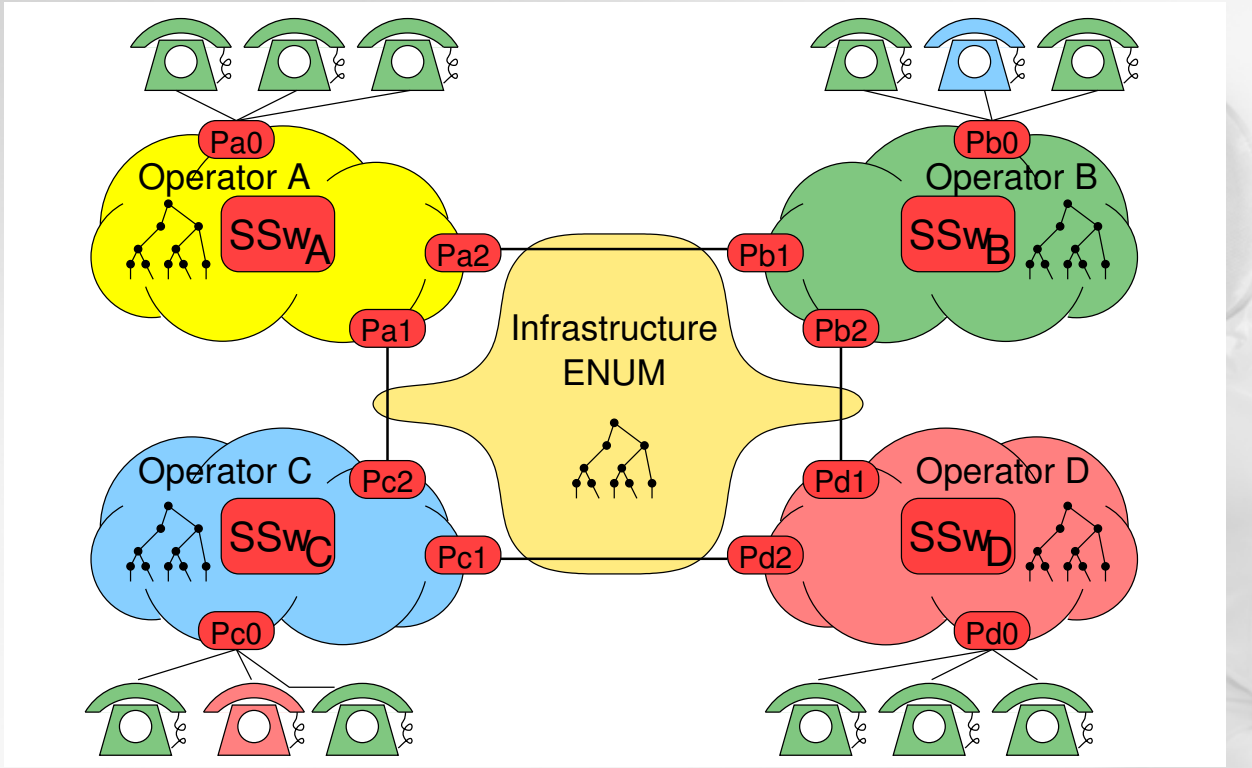
Annahmen

Vom öffentlichen Internet-DNS separates, „privates” ENUM/DNS
Verwaltet von einem Netzbetreiber, bzw. Betreiber-Konsortium
Abfrage aus Internet eingeschränkt bzw. unmöglich

Fragestellungen

Anwendbarkeit, Sicherheit von ENUM für „geschlossene" PlattformenKönnen Konzepte aus der SS7-Welt (z.B. Netzbetreiberkennungen, Rufnummernportierungsserver) angewendet werden?

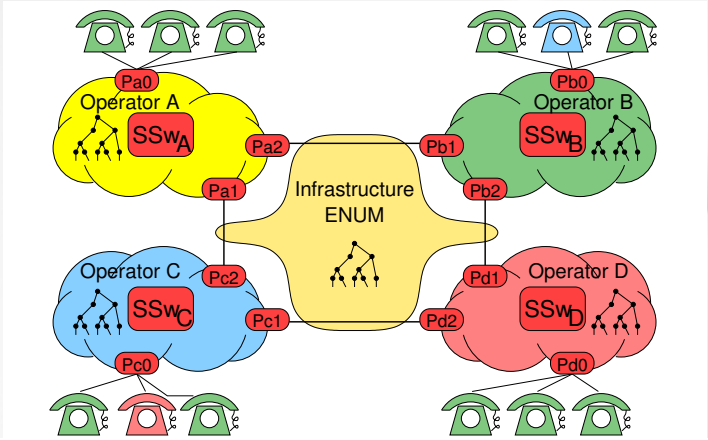
„Geschlossene“ SIP-Plattformen



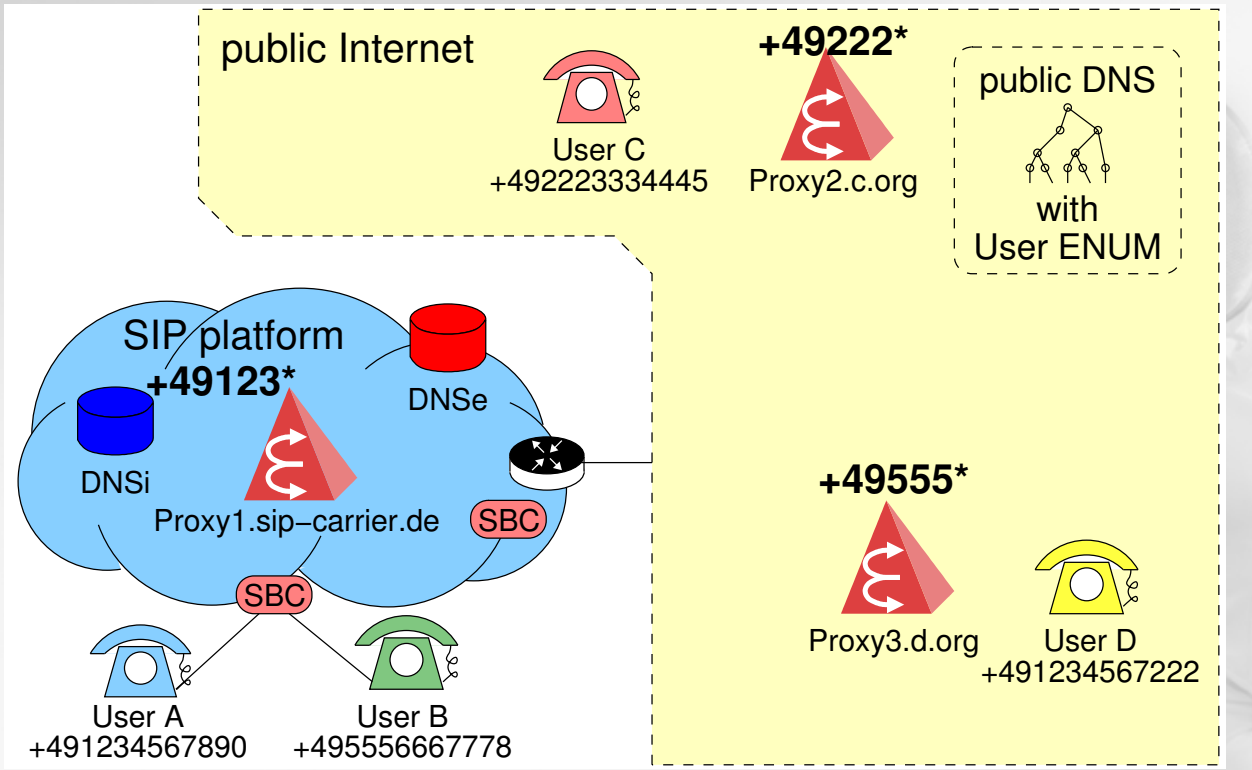
SIP-Interdomain Routing

Interdomain Routing zwischen geschlossenen SIP-Plattformen

- **Keine Ende-zu-Ende IP-Konnektivität**
  → Routing von SIP-Nachrichten zwischen Betreibern im Application Layer
  → Ggf. über Transit-Provider
  Medienströme hier nicht betrachtet
- **Zentrales Infrastructure ENUM (Betreiberkonsortium):**
  Rufnummer -> Netzbetreiberkennung (NBK)
- **SIP-Routing basierend auf NBK mit lokalem ENUM/DNS split horizon**
- **Zweistufige Auflösung über nicht-terminale Records möglich**



„Offene“ und „geschlossene“ Plattformen



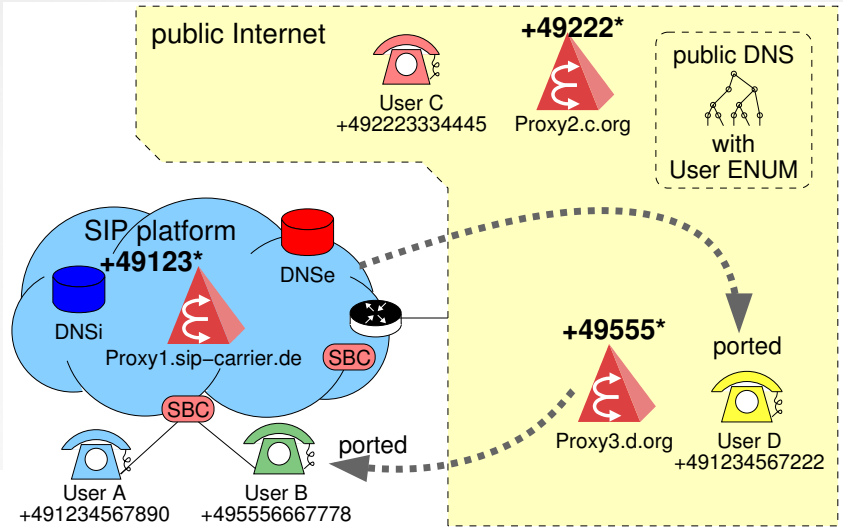
"Offene" und "geschlossene" Plattformen

Zusammenschaltung mit offenen SIP-Plattformen

■IP-basierte Interconnection zwischen SIP-Plattformen im Internet und geschlossenen Plattformen (über SBC)

Problemstellung

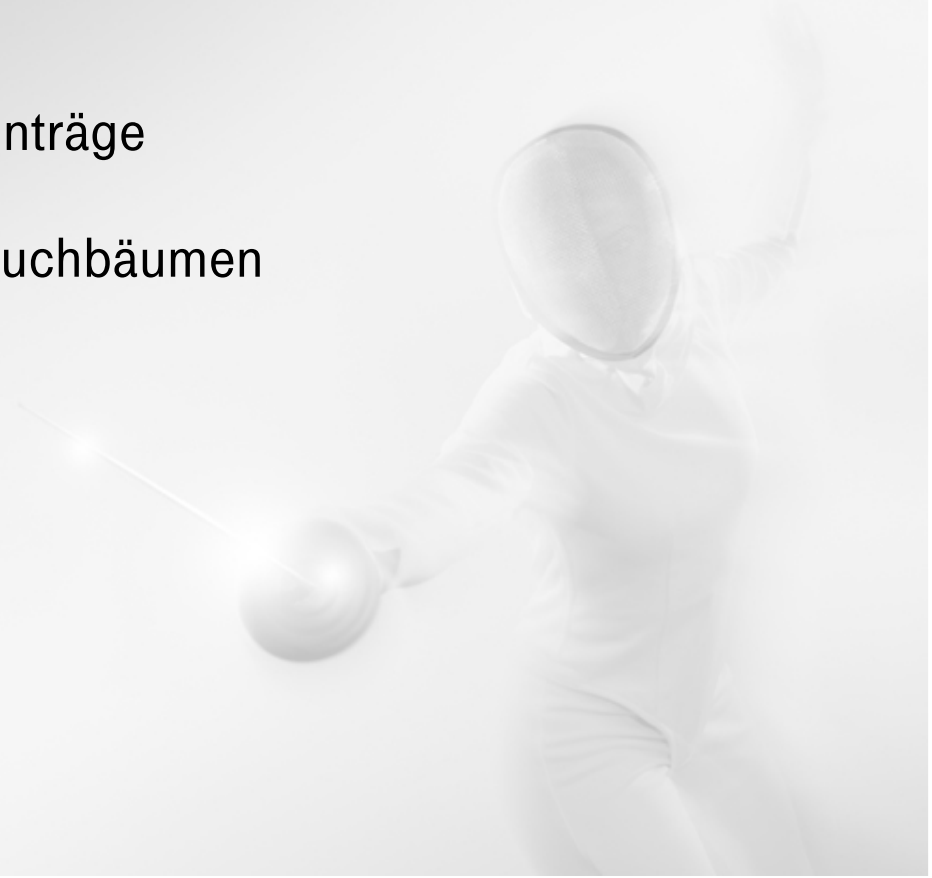
- Zugewiesene Rufnummerngassen
- Portierung von Teilnehmern
- Geschlossenen Plattform: Interne Calls unabhängig von User-ENUM



ENUM/DDDS

Offene / Geschlossene Plattformen:

- Eindeutigkeit der Zuordnung der Einträge
- Suchzeiten in den verschiedenen Suchbäumen
- Schleifenbildung



ENUM/DDDS: Schleifenerkennung

Nicht-terminale NAPTR records: Gefahr von Schleifenbildung

Beispiel

Nameserver „Carrier A“

```
*.1.9.4.external-carrier-enum.carrier-a.net. IN NAPTR 100 10 "" "E2U+sip"
"!^\+491(\d)(\d)$!\2.\1.1.9.4.external-carrier-enum.carrier-b.net.!" .

+49123 liefert 3.2.1.9.4.external-carrier-enum.carrier-b.net.(nicht-terminal)
```

Nameserver „Carrier B“

```
3.2.1.9.4.external-carrier-enum.carrier-b.net. IN NAPTR 100 10 "" "E2U+sip"
"!.*!3.2.1.9.4.external-carrier-enum.carrier-a.net.!" .

+49123 liefert 3.2.1.9.4.external-carrier-enum.carrier-a.net.(nicht-terminal)
```

→ DNS/ENUM/DDDS-Client in Endlosschleife!

Abhilfe: Zähler, Abbruch nach 5 nicht-terminalen Records
(draft-ietf-enum-experiences-03.txt)

ENUM/DDDS: Implementierbarkeit

Stand

- Spezifikation der weitergehenden Features des DDDS und dessen Anwendung mit ENUM zu komplex, unvollständig, fehlerhaft, widersprüchlich
- draft-ietf-enum-experiences-03.txt
  - Sammlung von Problemen und Fragen, wie z.B.
    - Verarbeitung von Order/Preference/nicht-terminalen RR
    - Schleifenbildung
    - Zeichensätze
  - Empfehlungen für Server- und Client-Verhalten
  - Vereinfachung und Beschränkung nicht-terminaler Regeln
- Im Test-/Wirkbetrieb meist nur einfache Umsetzungen
- ENUM/DDDS unterschiedlich implementiert
  - Einige Hardphones können z.B. nur 1:1 Umsetzung
  - SER kann z.B. nicht-terminale Regeln nicht verarbeiten
- IETF: Erneute/Verbesserte Spezifizierung von DDDS/ENUM fraglich

RR: Resource Record
SER: SIP Express Router

Zusammenfassung und Empfehlungen

- User-ENUM unter e164.arpa im offenen DNS
  - Abhängigkeit von Nameserverbetreibern und deren Sicherheit
  - DNSSEC löst Probleme, größere Verbreitung fraglich
  - Einträge prinzipbedingt öffentlich verfügbar
  - Vereinbarkeit mit klassischen Geschäftsmodellen?
- Empfehlungen
  - Eigene Infrastruktur möglichst unabhängig von User-ENUM gestalten
  - DNSSEC unterhalb 9.4.e164.arpa
- Infrastructure-ENUM für geschlossene Plattformen
  - Nicht-terminale RR für Interdomain-Routing grundsätzlich denkbar
  - (Einheitliche) Implementierung nicht-terminaler Records und deren Zukunft in den IETF-Standards unklar
- Empfehlungen
  - Ersatz nicht-terminaler NAPTR-RRs durch Mechanismen im Resolver, lokalen Nameservern, DNS-Provisioningsystem oder Datenbank
- Benutzer

  ISDN-Funktionalitäten sind integraler Bestandteil der Services, mit gelebten hohen Erwartungshaltungen der Benutzer, sowohl der Endkunden als auch der Serviceprovider

Unternehmenssicherheit T-Com