RIPE Meeting April 2006

Security Issues in ENUM

Gerhard Schröder

Deutsche Telekom, T-Com
Corporate Security

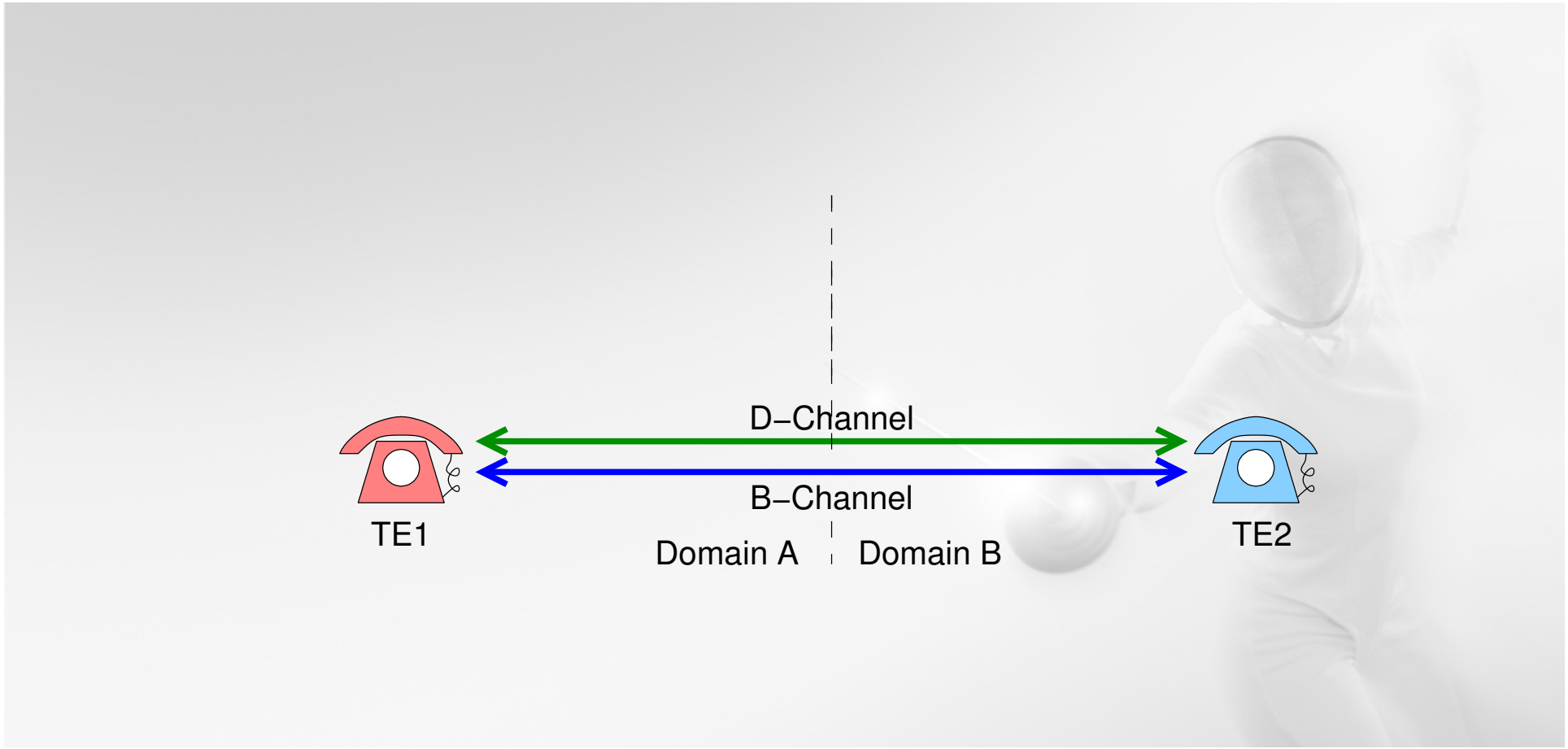
in Cooperation with
the University of Stuttgart

schroederg@t-com.net

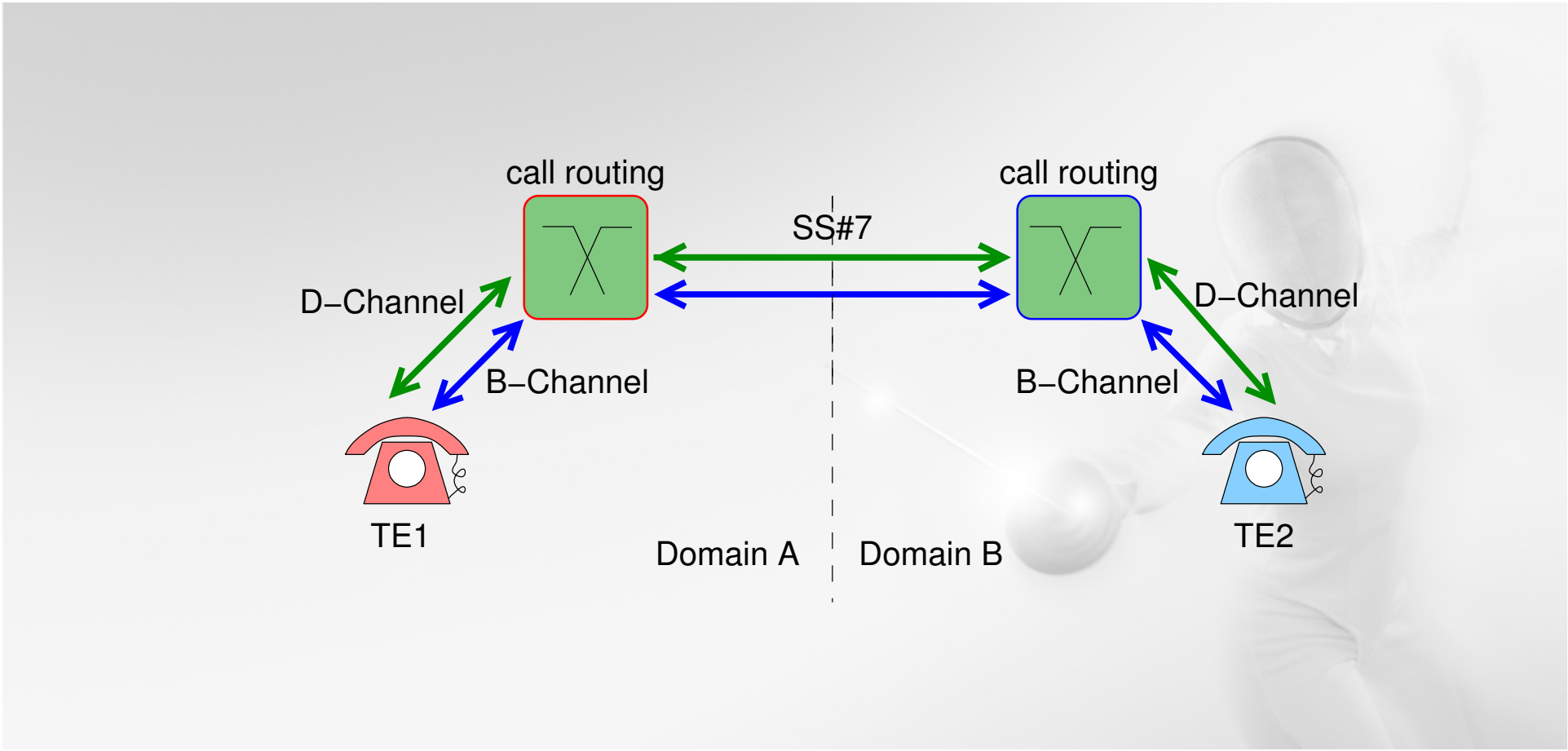
Security Issues in ENUM

- **Basics**
  ISDN, SIP
- **ENUM**
- **DNS**
  Security of the DNS-Infrastructure
  DNSSEC
- **Open and Closed SIP-Platforms**
- **Problems of Specification and Implementation of ENUM/DDDS**
- **Summary and Recommendations**

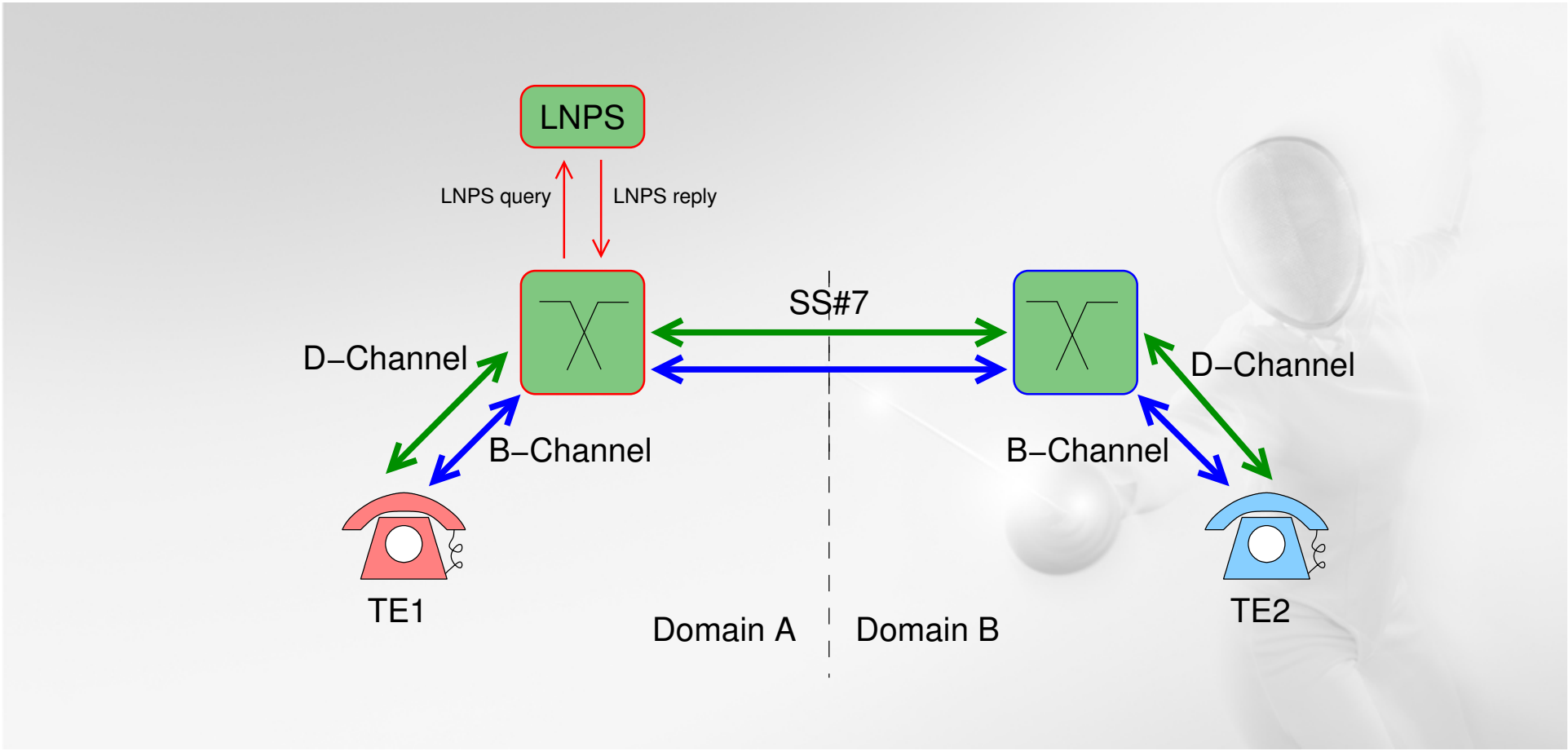
ISDN Connection (I)



ISDN Connection (II)



ISDN Connection (III)



ISDN Summary

Szenario: ISDN–Telephonie:

- Addressing of calling line numbers according to E.164
- Each MSN (Multiple Subscriber Number) is configured in a switch and mapped onto a fixed port.
- With testing the related D-Channel Parameters it is possible to verify whether the Calling Party Number is
  a) *network provided*
  b) *user provided and verified*
  c) *default*
- With this feature, a powerful mechanisms is given to verify and authenticate at the destination side the calling number of the caller.

ENUM and SIP

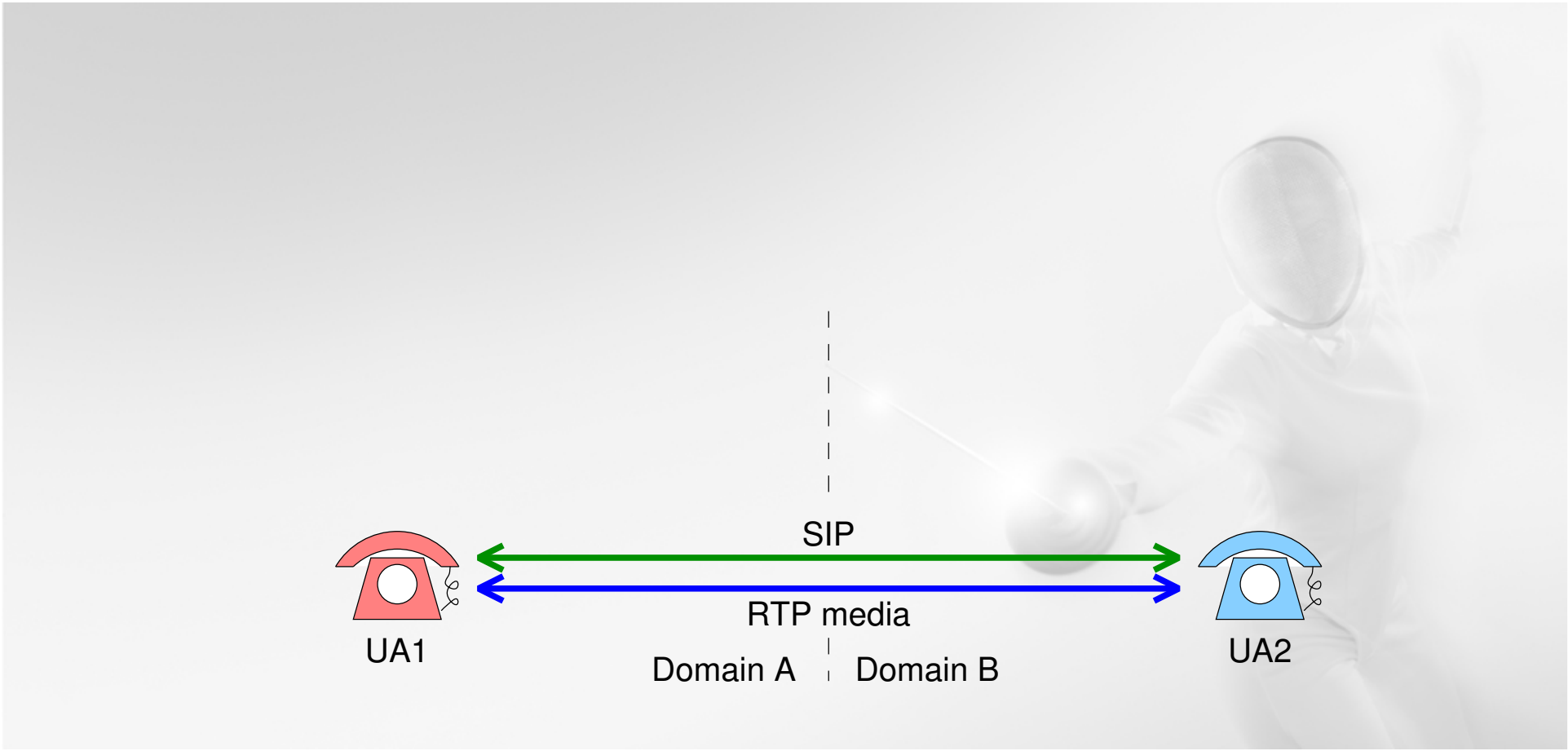
Scenario: IP-Telephony with SIP

Possibilities in addressing a subscriber:

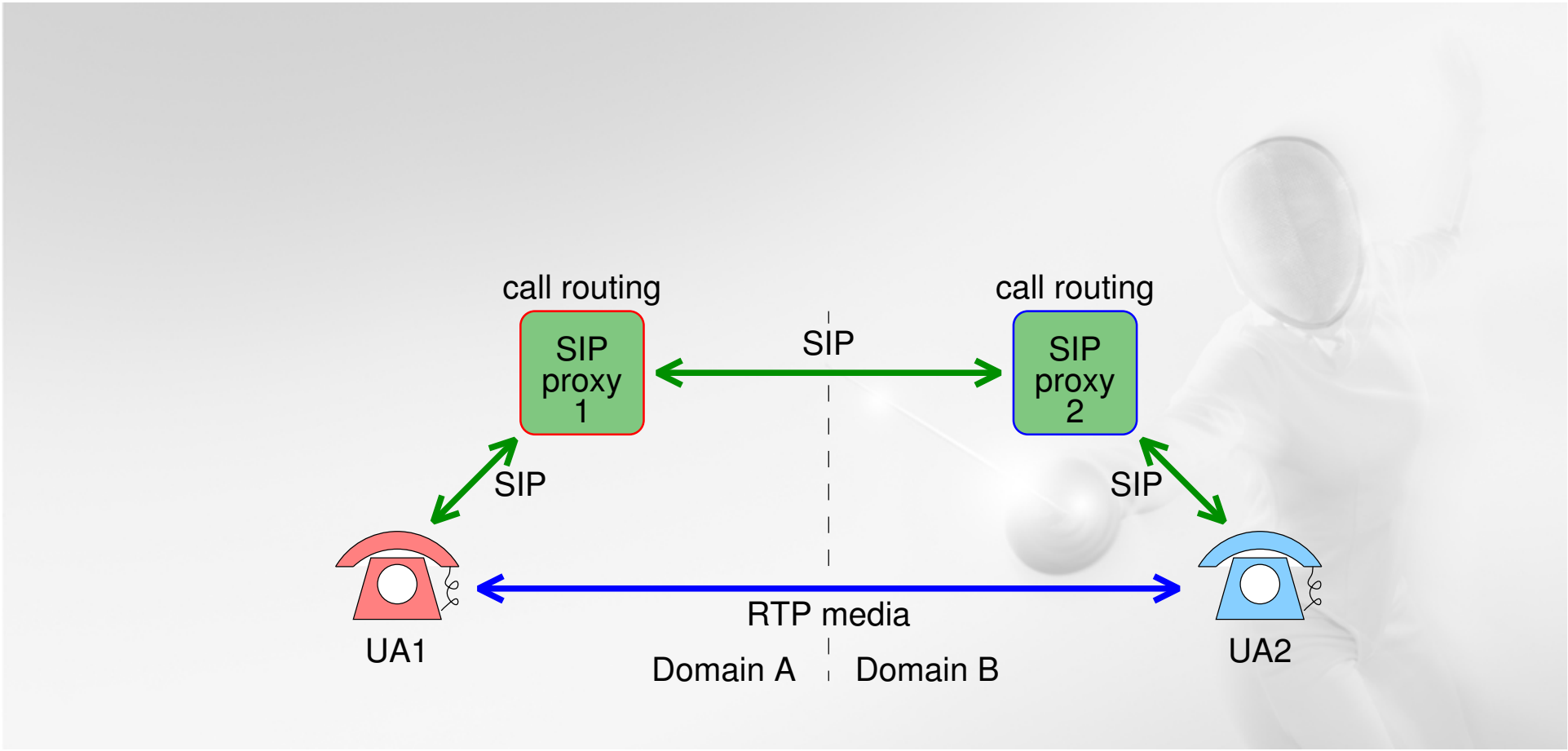
- **SIP URI / SIPS URI (Secure SIP = SIP over TLS)**
  localpart@domain, e.g. To: Alice <sip:alice@atlanta.example.com>
  it is also possible to specify a telephone number,
  Interpretation in accordance with the local guideline of the domain,
  e.g.: To: Jim <sip:+4961514711@sip-to-isdn-gateway.net>
- **TEL URI (Extension regarding RFC 2806)**
  International Telephone number according to E.164,
  To: Jim <tel:+49-6151-4711>
- Desirable, for reusing of well-known numbers
  Necessary with Interconnection of ISDN (TE can deal digits only)
- **SIP Implementations have to support SIP und SIPS, only**

Target:
ENUM: Converting E.164 → SIP URI (or others) by utilising the DNS

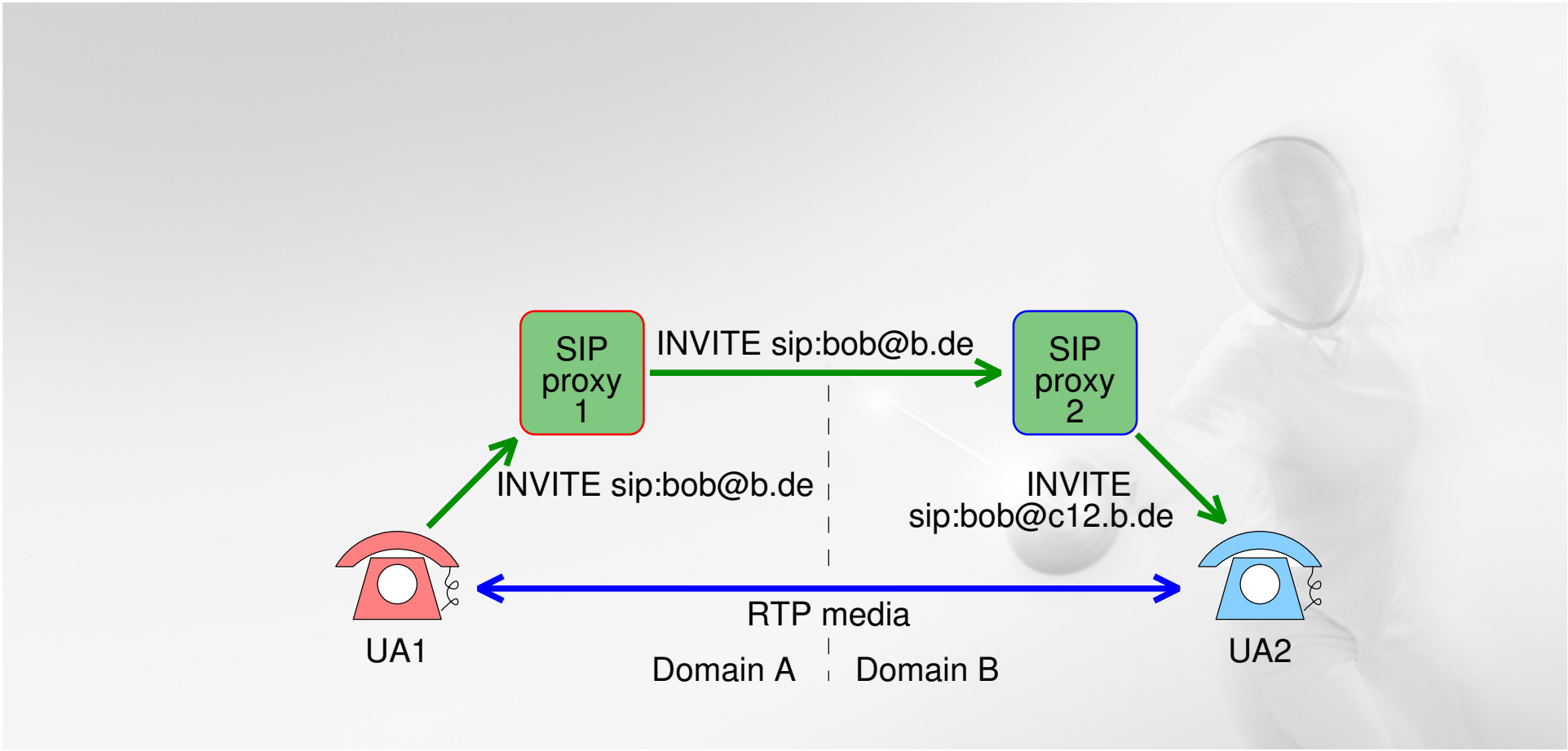
ENUM and SIP (I)



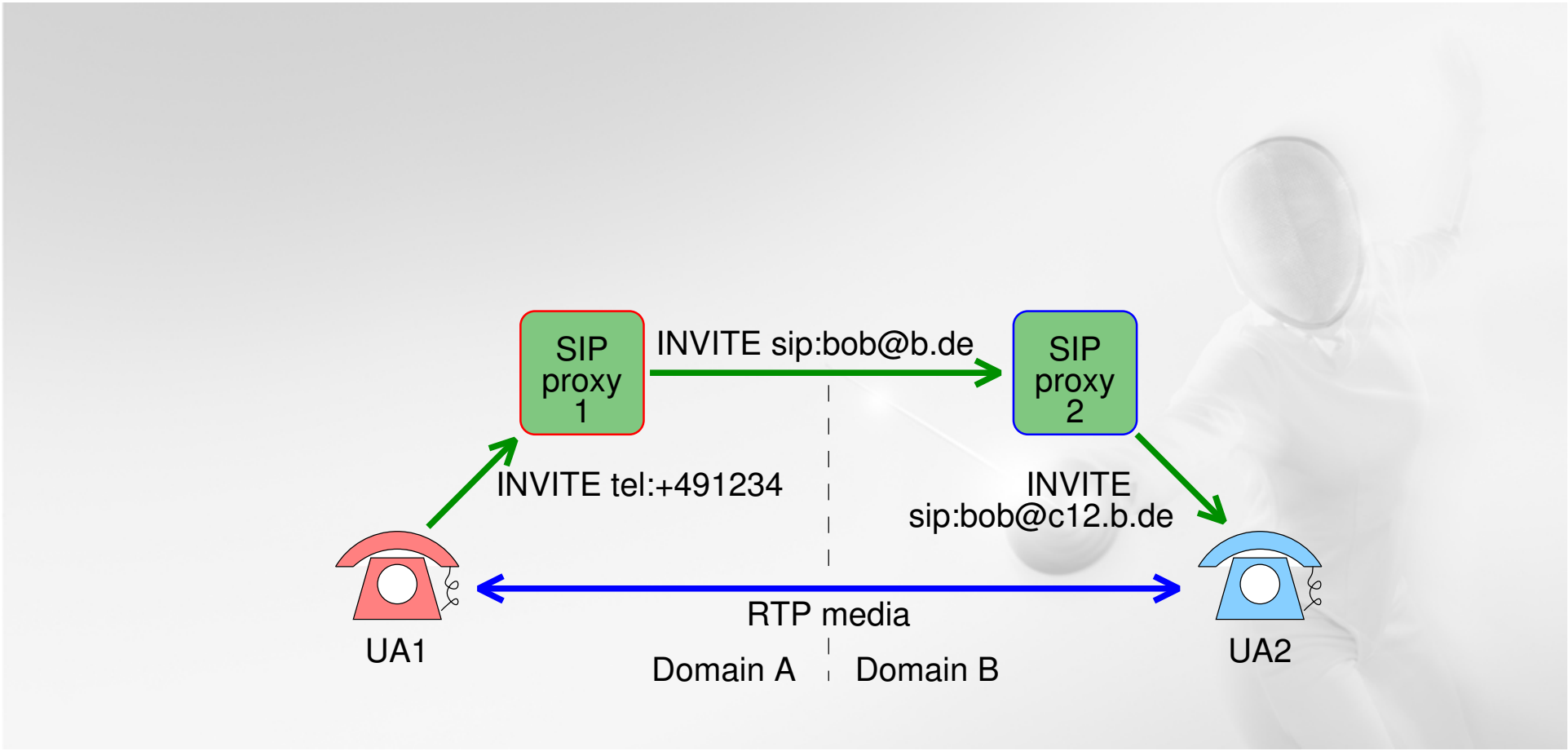
ENUM and SIP (II)



ENUM and SIP (III)

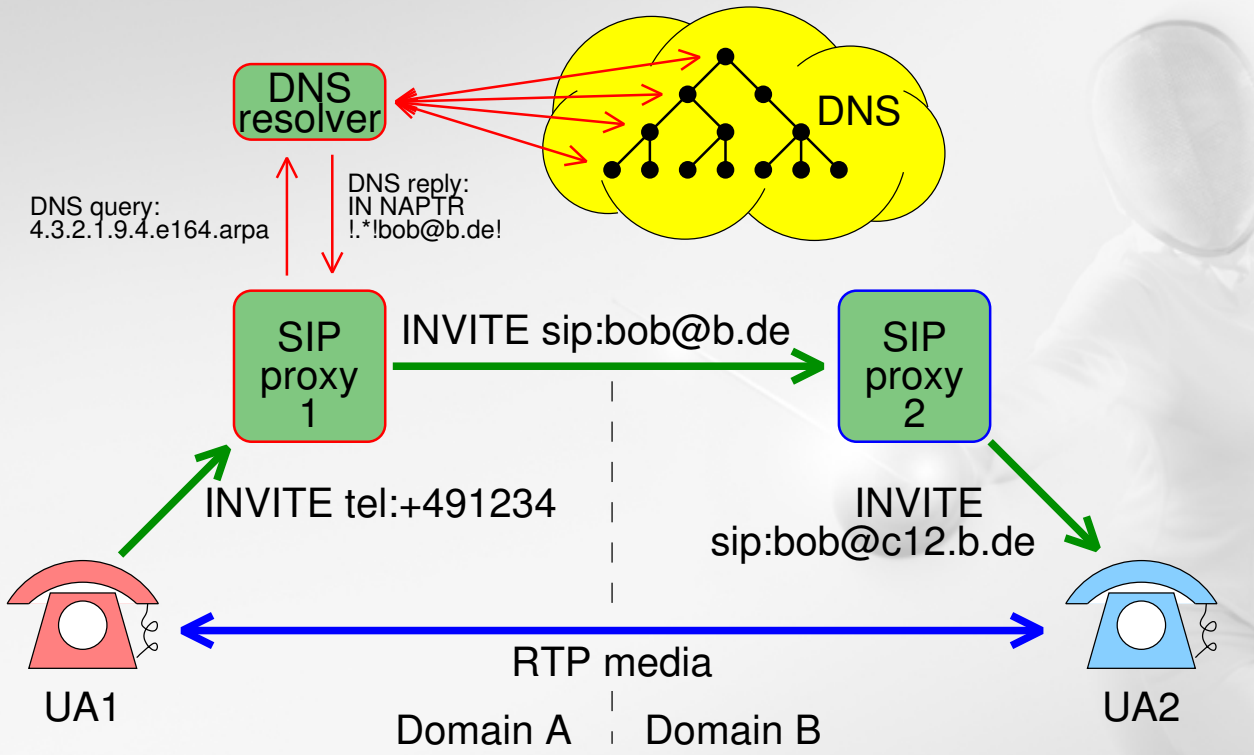


ENUM and SIP (IV)



ENUM and SIP (V)

Target ENUM:
Converting E.164 → SIP URI (and others) by utilising the DNS



ENUM Standardisation

Target ENUM:

Converting E.164 → SIP URI (and others) by utilising the DNS

- **RFC 2916 (09/2000): E.164 number and DNS**
  First RFC for ENUM
  20 Pages
  Registration and Search of E.164-Nummern in the DNS, NAPTR record
  Replaced by RFC 3761
- **RFC 3401 - 3406 (10/2002): Dynamic Delegation Discovery System**
  Generalised Concept for generic address mapping
  DNS is one solution among other (theoretically possible) databases
  Not all concepts are completely mature
- **RFC 3761 (04/2004): ENUM as an application of the DDDS**
  Together with the DDDS specification: 105Pages

ENUM Scenarios

- **Consideration of the mapping on auf DNS server structures for "open" Scenarios**
  Dependencies from external Naming Server Operators
- **Analysis of alternative network configurations: „closed" SIP Platforms**
  From the public Internet-DNS separated private „Infrastructure ENUM"
  Scenarios for Interdomain -Routing
  Using of non-terminal roles
- **Connection of open and closed platforms**
  Mixed-Scenarios consisting of Infrastructure ENUM (for network internal calls) and User ENUM (for calls to and from other networks)
  Minimal requirement: Ensure at least network internal calls

ENUM-Configuration „open network”

- **RFC 3761**
  ENUM-entries for public E.164-Nummern below the DNS root „e164.arpa.”, in the public Internet-DNS visible
  ENUM/DDDS-Mechanism can be used below other roots, but it is not allowed to call it in this case ENUM
- **DENIC eG**
  ENUM-Trial till December 2005,
  9.4.e164.arpa. (currently) delegated to DENIC
  Direct registration of single calling numbers of end customers
  this is line with the registration for .de-Domains
  NAPTR-data records are visible worldwide in the Internet
  → Approach “open Internet”
  E.164-number allocation separated from network access / transport service
  DNS-Infrastructure supports to find an UA, the rest: End-to-End
  → Problems: data protection, DoS-attacks , VoIP-Spam, ...

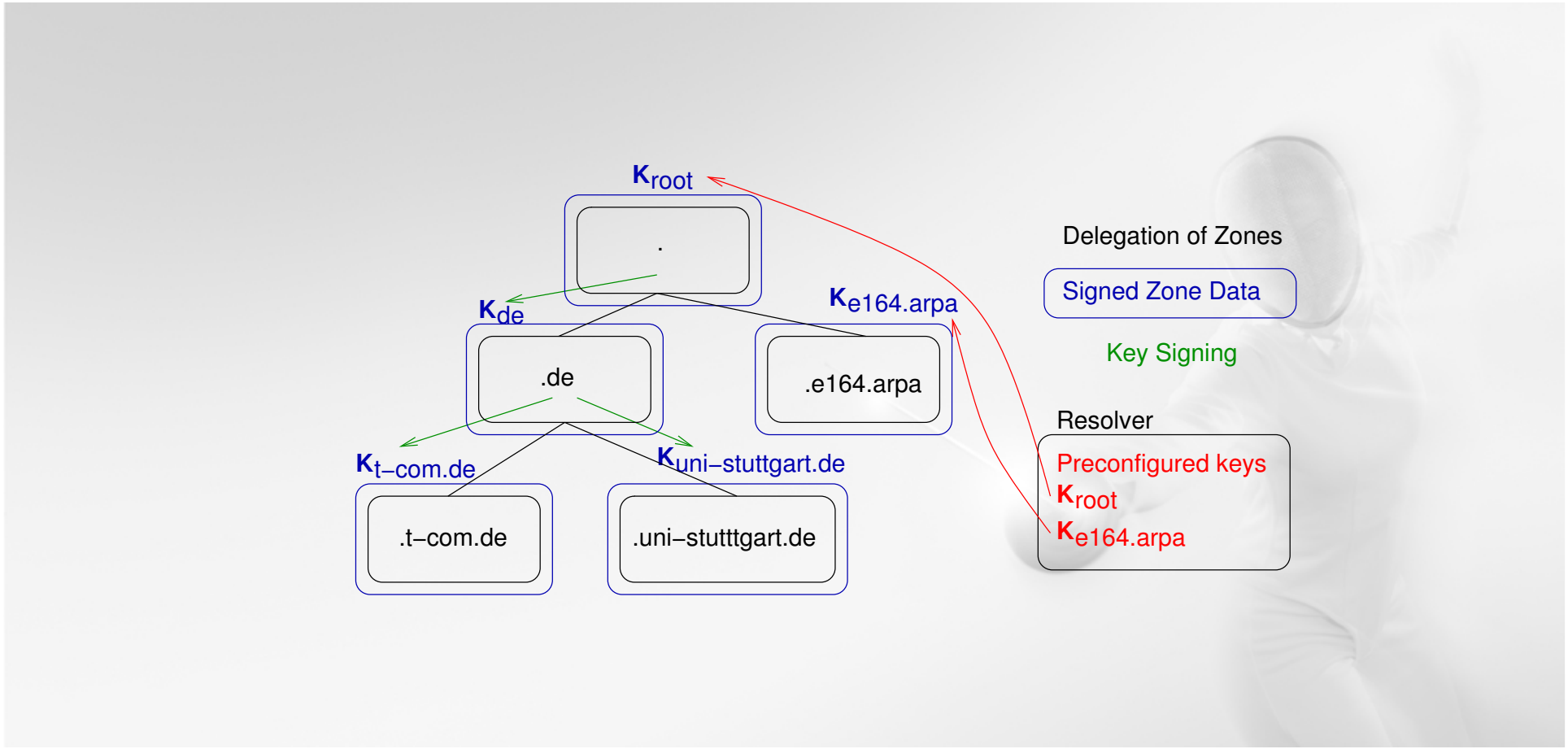
Analysis of DNS server structure

Problems of DNS server structure

- **Integrity of queries**
  A compromised or misconfigured Server in the tree
  → Wrong response on an DNS query
  Taking advantages of weaknesses in the implementation and in the LAN
  DNS Cache Poisoning
  DNS Spoofing

- **Proposed solution: DNSSEC**
  DNS Security Extensions RFC4033-4035 (März 2005)
  Protection of the integrity of DNS-entries with digital signatures
  pre-configured public keys in resolvers (Trust Anchor)

DNSSEC



DNSSEC

Questions about DNSSEC

- **Administrative Problems of a global PKI**
  Distribution of new (Root-) keys
  → How to replace pre-configured keys in the resolver?
  Signature of keys for each new delegated zone necessary
  Change of keys requests also a modification in the higher-ranking zone
- **Some weaknesses still exists**
  Sensivity against DoS Attacks
  Weaknesses in the implementation
- **Protecting the confidentiality of the entries not possible**
  This method is based on established DNS
  However, in particular important for ENUM

DDDS Regular Expression

Plain implementation

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

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

→ **Capabilities of Regular Expressions are not used**

Implementation of number ranges

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

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

“Closed” SIP-Platforms

Analysis of alternative network structures

- **„CLOSED” SIP Platforms**
  e.g.: ETSI TISPAN, 3GPP IMS
  No or limited End-to-End IP connectivity
  Session Border Controller (Firewalls)
  → Application Layer - Routing-Mechanism (...Interdomain) necessary

Assumptions

From the public Internet-DNS separated „private” ENUM/DNS
Managed by a carrier or a group of carriers
Request from the Internet limited or not possible

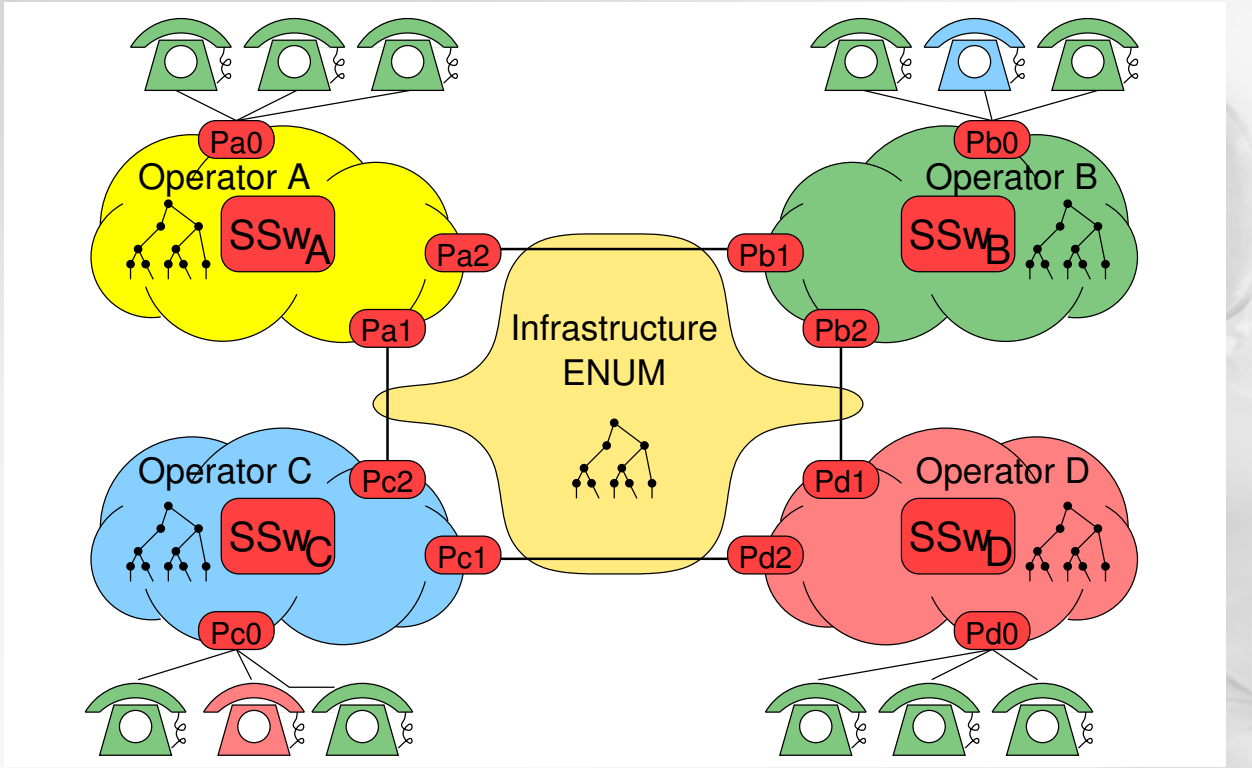
Questions

Applicability and Security of ENUM in „closed" Platforms

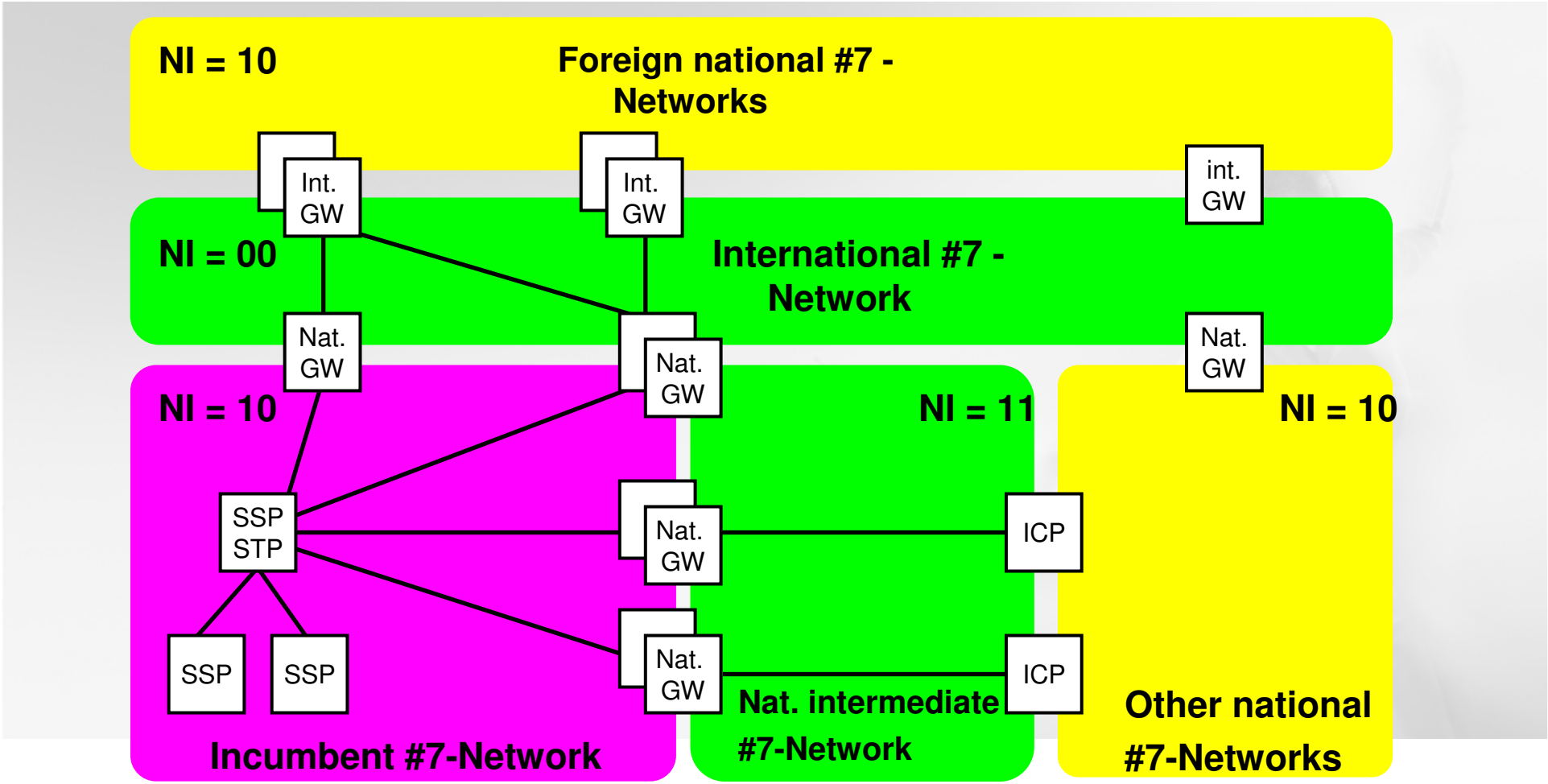
May concepts from the SS7-world (like Carrier-ID’s, LNPS) be applied?

T-Com

“Closed” SIP-Platforms



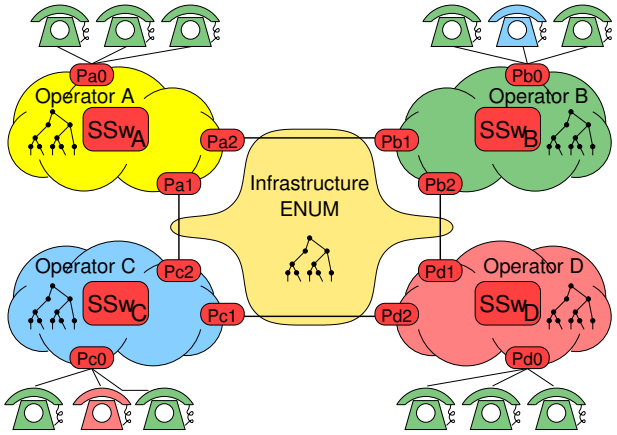
Network Structure: #7-Network



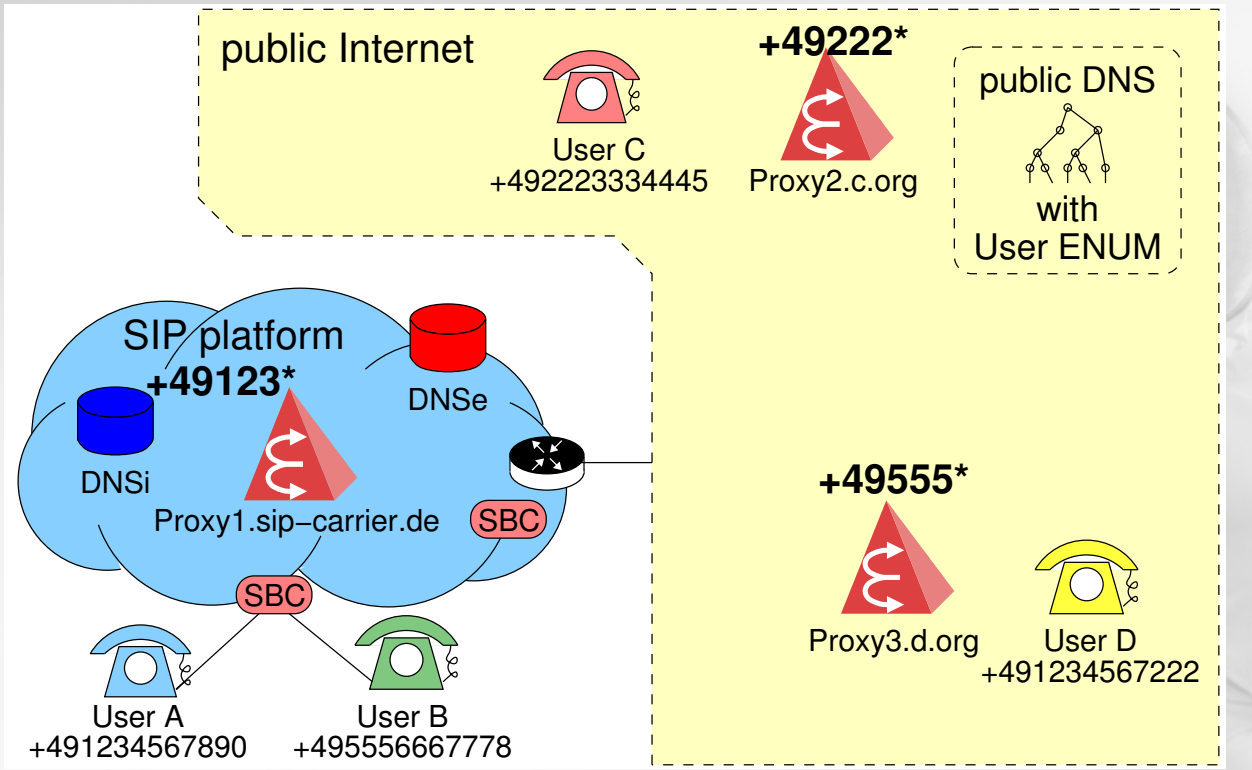
SIP- Interdomain Routing

Interdomain Routing between closed SIP-Platforms

- **No End-to-End IP-Connectivity**
  → Routing of SIP-messages between Carrier on an Application Layer
  → if necessary via Transit-Provider
  Media streams not considered here
- **Centrale Infrastructure ENUM (Group of Carrier):**
  Calling number -> Carrier ID
  SIP-Routing based on Carrier ID with local ENUM/DNS split horizon
- **Two-step resolution possible via non-terminal records**



„Open“ und „closed“ Platforms



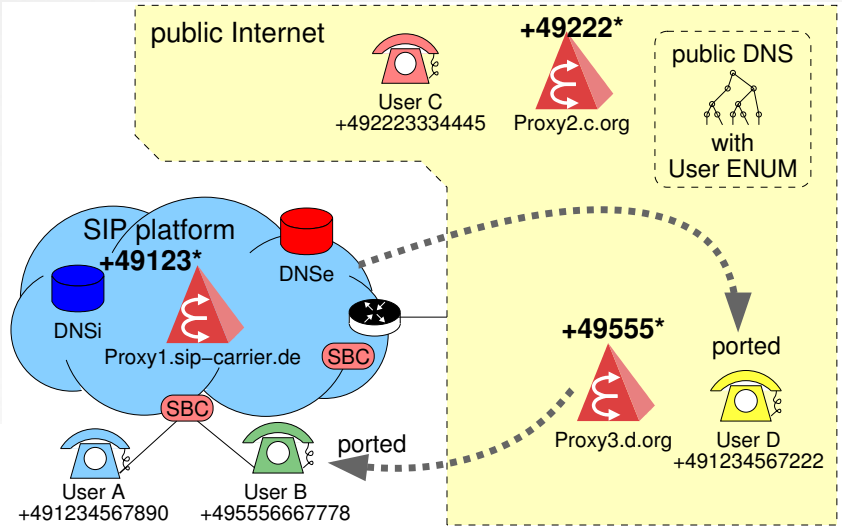
“Open" und “Closed" Platforms

Interconnection of open SIP-platforms

- IP-based Interconnection between SIP-Platform inside the Internet and closed platforms (via Session Border Controller SBC)

Problems:

- Assigned calling number ranges
- Porting or transferring of customers
- Closed Platforms: Internal Calls independent from User-ENUM



ENUM/DDDS: Recognition of loops

Non-terminal NAPTR records: Risk in creating loops

Example

Name server „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 delivers 3.2.1.9.4.external-carrier-enum.carrier-b.net.(non-terminal)

Name server „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 delivers 3.2.1.9.4.external-carrier-enum.carrier-a.net.(non-terminal)

→ DNS/ENUM/DDDS-Client in an infinite loop!

Remedy: Introduction of a counter, stop after 5 cycles
(draft-ietf-enum-experiences-03.txt)

ENUM/DDDS: Implementability

Status

- **Specification of further features of DDDS and their usage for ENUM is very complex, incomplete, incorrect, contradictory**
- **draft-ietf-enum-experiences-03.txt**
  - Collection of problems and questions, e.g.
  - Processing of order/ preference/ non-terminal Resource Records
  - Loops
  - Character Sets
  - Recommendation for Server- and Client behaviour
  - Simplification and Restricting of non-terminal roles
- **In test and field environment mostly plain implementation**
- **ENUM/DDDS implemented differently**
  - Some hard phones can only perform 1:1 conversions
  - SER e.g. can not process non-terminal roles
- **IETF: Re-examining or improvement of the specification open (doubtful)**

RR: Resource Record
SER: SIP Express Router

T-Com

Summary and Recommendations I

- **User-ENUM below e164.arpa as part as the open Internet DNS**
  - Dependency on name server provider and their security measures
  - DNSSEC solve some problems, but a large propagation is still open
  - In principle, entries are public available
  - Compatibility with classical business not clear yet

- **Recommendations**
  - Creating an own infrastructure, if possible independently from User-ENUM
  - DNSSEC below 9.4.e164.arpa (for Germany)

Summary and Recommendations II

- **Infrastructure-ENUM for closed platforms**
  - Non-terminal RR for Interdomain-Routing in principle imaginable
  - (Uniform) Implementation of non-terminal records and their future in the IETF-Standards is still an open issue.
- **Recommendation**
  - Replacement of non-terminal NAPTR-RRs with mechanism in the Resolver, locale name server, DNS-Provisioning system or databases.
- **Customer**
  As far as telephony services are concerned, the customers as well as the service provider expects a service with high quality and high reliability. All of them have learned from their experience with the PSTN/ISDN.

Colophon

All statements in this presentation results from a project to analyse the security issues of ENUM. Among others, one focus was a comparison with PSTN.

In the presentation no statements about the technology strategy of Deutsche Telekom T-Com are given.