

# VoIP and CLI

## Trusted Identification

---

**RIPE 46**

**VoIP and ENUM Tutorial**

**1. September 2003**

**Richard STASTNY**

ÖFEG/TELEKOM AUSTRIA, Postbox 147, 1103-Vienna

enum: +43 664 420 4100

E-Mail: [richard.stastny@oefeg.at](mailto:richard.stastny@oefeg.at)

[richard@stastny.com](mailto:richard@stastny.com)

# Today's Roadmap on Numbering

---

1. POTS – from Comfort to Numbering
  - Why are the numbers in the PSTN in the way they are?
  - A History
2. ENUM and VoIP – Numbering and Dialing Plans
  - ENUM Mapping of E.164 Numbers to Internet Names and Addresses
  - E.164 Numbers for VoIP and Routing on the PSTN
  - Numbering and Dialing Plans for VoIP
  - An Overview and a Proposal
3. VoIP and CLI – Trusted Identification
  - Calling Line Identification on VoIP
  - A Proposal

# Calling Line Identification

---

- Numbers are also used for CLI
- the CLI serves different purposes:
  - Call back information to the called user (as dial string)
  - Identification of the user and his location to emergency services and for legal intercept
  - Identification of the user for malicious call identification (MCI)
  - Identification of the user for accounting purposes (e.g. carrier selection)
- In the PSTN the CLI is tagged with
  - a Screening Indicator (SI) and
  - a Presentation Indicator (PI) set by the user (CLIR)
- In the PSTN all networks are in a Circle of Trust
  - so the information is transmitted via all Network-Network Interfaces (NNI) and is withheld on most User-Network-Interfaces (UNI) (except emergency services) if requested by the PI

# CLI in the PSTN

---

- In the PSTN the CLI is tagged with a screening indicator:
  - network provided,
  - user provided, verified and passed
  - user provided, unscreened
    - This information is set by the calling party and is neither screened by the PBX or by the switch, if transmitted via the User-Network-Interface. It is always replaced by the switch with the **network provided number** in the calling party identification. Only if there is the possibility of transmitting a second CLI as **generic number**, this information is transmitted IN ADDITION.
- The subscriber may request with a (mandatory) supplementary service (CLIR) (permanent or call-by-call) that the presentation of the network provided number is restricted with the PI
  - presentation restricted
  - presentation allowed

# Trust Circle

---

- PSTN networks are able to rely on this information because they trust each other
- To extend this trust to VoIP and the Internet, the following is necessary:
  - Network-network-Interfaces between the PSTN and the Internet (SS7 Gateways), because on UNIs always the network provided number is inserted
  - A Circle of Trusted VoIP service providers (SP)
  - Secure signaling between the servers operated by the SP
  - Proper identification of subscribers and authentication of users
  - properly assigned E.164 numbers
  - Secure signaling between users and servers
- See work on SIM card authentication, trusted Remote Party IDs and network asserted identities (NAI)

# Reliable CLI of E.164 Numbers on VoIP

---

1. E.164 Number provided by service provider
  - Currently the normal case
  - may be implemented immediately
  - Identity of subscriber held by service provider
2. E.164 number provided by user
  - requires E.164 certificates
  - allows in connection with accounting certificates ad-hoc or call-by-call subscription
  - may be implemented later in addition
  - Identity of subscriber held by E.164 number issuer or credit card company

# E.164 Number provided by Service Provider

---

- The user **MUST** have a subscription with a VoIP SP with proper identification
- The E.164 number **SHALL** be either assigned by the VoIP SP or ported in by the subscriber (**REQUIRES** proper validation or certificate)
- The user **MUST** register by the VoIP SP in a secure manner
- The user is setting up a call via secure signaling and **MUST** be able to indicate the VoIP SP if the presentation of his identification (the E.164 number) to other users **SHALL** be restricted (CLIR)
- The VoIP SP **SHALL** send this identification only to trusted partners and only via secure signaling (e.g. TLS or VPN).
- The user **MAY** set up a different identification as user provided
- If the trusted partner is a gateway to the PSTN, the gateway **SHALL** set up the trusted identification as network provided and set the proper Presentation Indicator (this requires SS7 Signaling)
- The gateway **MAY** in addition set up the user provided identification as generic number, if available.
- A trusted partner **MUST** withhold the transmission of the identification to a UA or an untrusted service provider (proxy) if presentation is restricted
- If a communication to an untrusted partner is established, only the user provided information **SHALL** be delivered if the presentation is restricted.
- In case of law enforcement, the identity of the user (subscriber) holding the E.164 number **MUST** be retrievable from the VoIP service provider

# E.164 Number provided by User

---

- The user **MUST** have a E.164 Number assigned by a certified entity and also **MUST** have a certificate showing the right to use this number
- The user **MAY** have a subscription with a VoIP SP, but **MAY** also subscribe ad-hoc
- The user **MUST** register by the VoIP SP in a secure manner providing his certificate.
- The user is setting up a call via secure signaling and **MUST** be able to indicate the VoIP SP if the presentation of his identification (the E.164 number) to other users **SHALL** be restricted (CLIR)
  - The VoIP SP **SHALL** send this identification only to trusted partners and only via secure signaling (e.g. TLS or VPN).
  - The user **MAY** set up a different identification as user provided
  - If the trusted partner is a gateway to the PSTN, the gateway **SHALL** set up the identification as network provided and set the proper Presentation Indicator (this requires SS7 Signaling)
  - The gateway **MAY** in addition set up the user provided identification as generic number, if available.
  - A trusted partner **MUST** withhold the transmission of the identification to a UA if presentation is restricted
  - If a communication to an untrusted partner is established, only the user provided information **SHALL** be delivered if the presentation is restricted.
- In case of law enforcement, the identity of the user (subscriber) holding the E.164 number **MUST** be retrievable from the entity assigning the E.164 Number



# Proposal

---

- It is proposed to set up a global field trial for exchanging trusted CLIs
- This requires:
  - creation a Circle of Trust between (some) of the ITADs currently interworking already in VoIP and ENUM
    - Note: this does not prevent communication with "untrusted" entities (on the contrary, you just have to stick with the rules)
  - establishing a secure communication between the trusted entities
  - some entities should provide SS7 based interworking with the PSTN/ISDN
  - Trusted entities need to get access to genuine E.164 numbers
  - Trusted entities need to identify their subscribers

# The End

---

**Thank you for  
your attention**