SIP Extensions for Caller Privacy

W. Marshall, K. K. Ramakrishnan, E. Miller, G. Russell, B. Beser, M. Mannette, K. Steinbrenner, D. Oran, J. Pickens, P. Lalwaney, J. Fellows, D. Evans, K. Kelly, F. Andreasen

AT&T, CableLabs, 3Com, Cisco, Com21, General Instrument, Lucent Cable, NetSpeak, Telcordia

July 1999

IETF Presentation

Calling Identity - PSTN

- Calling Identity items
  - Calling Number
  - Calling Name
- Terminating switch must be able to identify calling party, e.g. for call trace, thus calling party identity must be passed.
- Calling Identity Delivery services allow the called party to obtain calling identity information about the calling party
  - MUST be able to trust validity of information delivered
  - PSTN is trusted intermediary
- Calling Identity Delivery Blocking (CIDB) features allow the calling party to control the presentation of calling identity items
  - MUST be able to trust that calling identity information is not revealed
  - PSTN is trusted intermediary

Calling Identity - SIP

- From header may be encrypted for privacy or other reasons
  - Cannot be modified since part of CallId (but display-name can)
- Calling identity delivery - use “display-name” in From header field:

  `name-addr  = [ display-name ] "<" addr-spec ">”`

  however SIP User Agents residing on customer premise cannot be trusted => need for trusted intermediary
- DCS-Proxy is the trusted intermediary
  - Ensures “display-name” provided by User Agent is valid.
  - Adds “display-name” when not provided by User Agent to enable call trace
- If the User Agent wants to suppress calling identity delivery:
  - UA could do this implicitly by not providing it to the DCS-proxy (but DCS-proxy still needs to support call trace), or
  - Explicitly indicate that calling identity is to be suppressed with a new header

Calling Identity - SIP, cont.

- To maintain complete privacy and anonymity, it must be possible to suppress all location information:
  - IP-addresses
    - » Some IP-addresses may be mapped to approximate physical location
    - » The fact that an IP-address used is different from what it normally is may reveal location information, e.g. working from home versus in office.

- Thus, Calling Identity items include:
  - Calling Number
  - Calling Name
  - IP-address

IP address privacy

- IP-address hiding needs a level of indirection by a trusted intermediary (anonymizer).

- DCS-proxies must be told to maintain IP-address level privacy

- New header field Privacy proposed to signal this:

```
Privacy     = "Privacy" ":"  *privacy-tag

privacy-tag = "Full" | "Caller-Num" |
                  "Caller-Name" | "IPAddr"
```

Privacy - Other Issues to Consider

- From header field
  - » May be encrypted.
  - » Set “display-name” to anonymous before forwarding to User Agent.
- Contact header field
  - » Point to anonymizer
- Via header fields
  - » May be encrypted or removed statefully by proxies
- Call-ID
  - » Should not be based on endpoint’s IP-address
- SDP
  - » Several fields include IP-address and user information, e.g. owner
- RTCP
  - » Some messages may include user information, e.g. NAME