HACK IN BO
Winter 2025 Edition
25ª EDIZIONE

VoIP Security: vulnerabilità e hardening

Davide Rasoli

Tecnico VoIP @ Com.tel S.p.A.

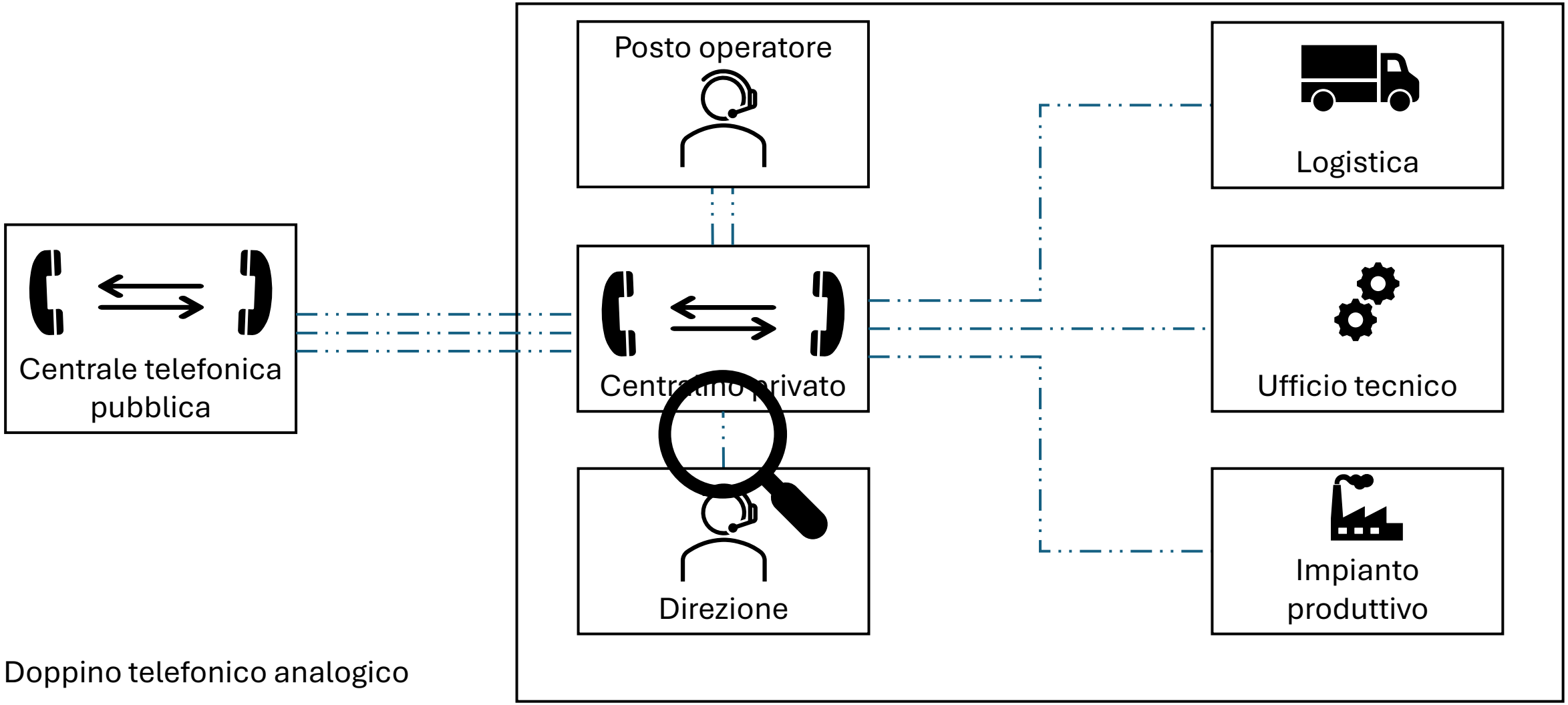
LinkedIn: /in/davider144

Agenda

HACK IN BO® Winter 2025 Edition
25ª EDIZIONE

1	Telefonia e sicurezza… Da sempre un rapporto difficile.
2	I concetti base del VoIP, un piccolo passo avanti.
3	Implementazione minimal: quali rischi si corrono?
4	Mettere in sicurezza il proprio sistema telefonico.
5	Di chi non dobbiamo fidarci. CLI Spoofing e mitigazione.

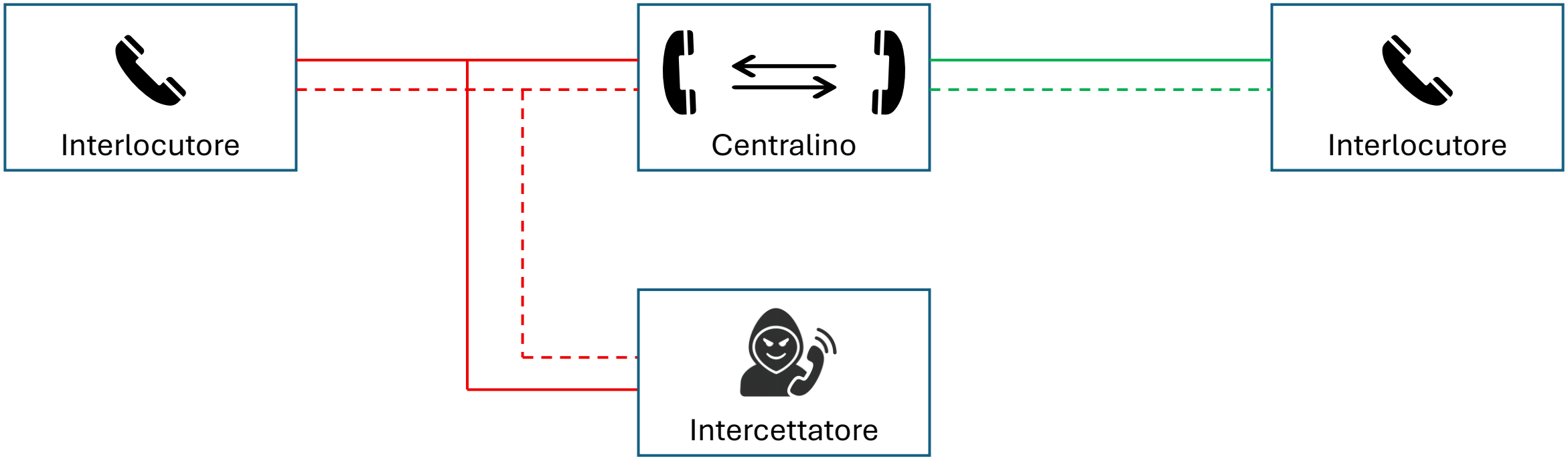
La semplicità delle linee analogiche



Telefonia e sicurezza... Da sempre un rapporto difficile.

Intercettazione su doppino analogico

- Il doppino analogico ha una composizione molto semplice: due conduttori elettrici.
- La nostra voce viene trasmessa sotto forma di differenza di potenziale tra i due conduttori.
- Tutto dipende dalle porte del centralino, e di conseguenza dal doppino.
- Non solo voce, anche dati (macchine FAX).

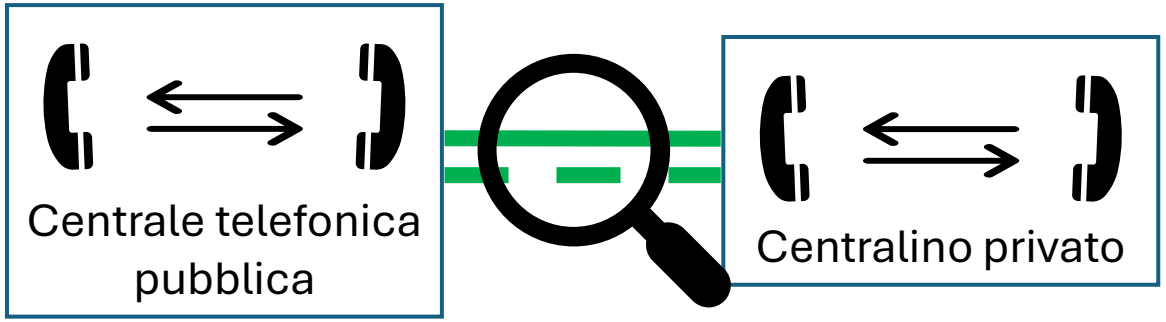


Telefonia digitale

La tecnologia evolve… Ma la sicurezza non migliora.

Basata su:

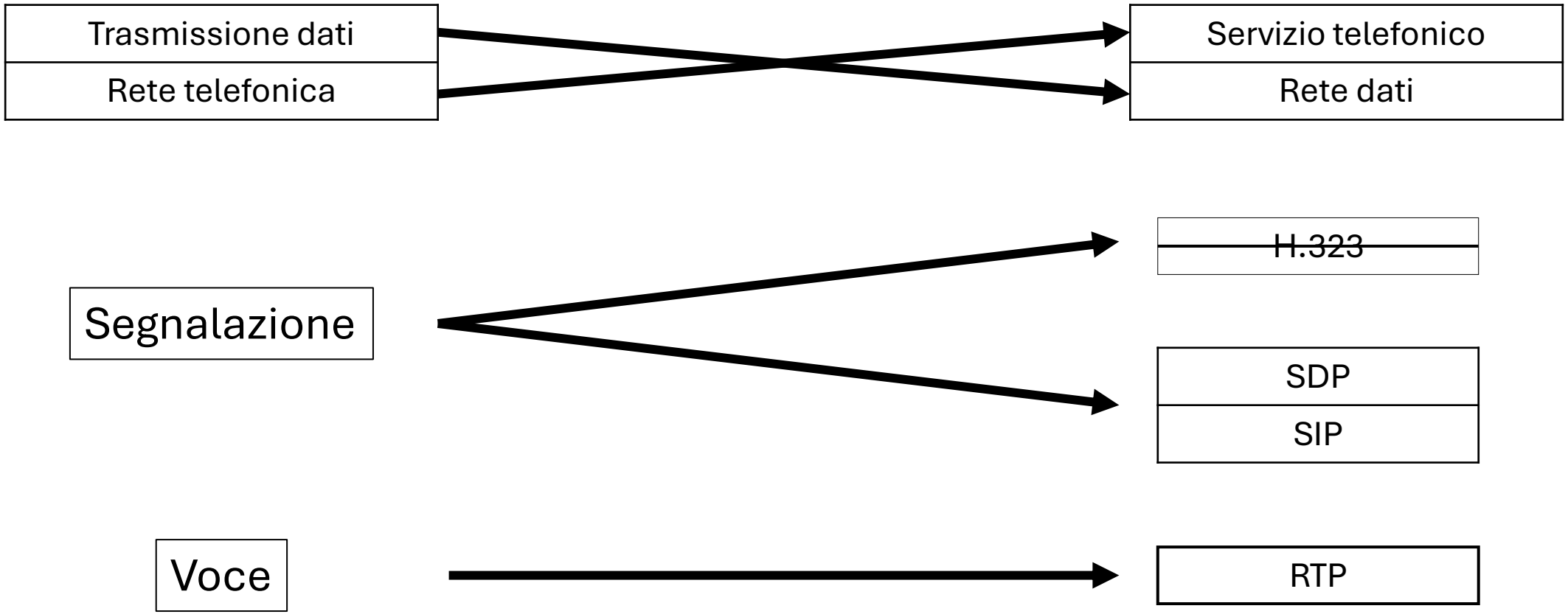
- Time division multiplexing
- Segnalazione e trasmissione dati su canali separati



Il cavo (fisicamente parlando) inizia a perdere l’importanza che aveva.

Telefonia VoIP

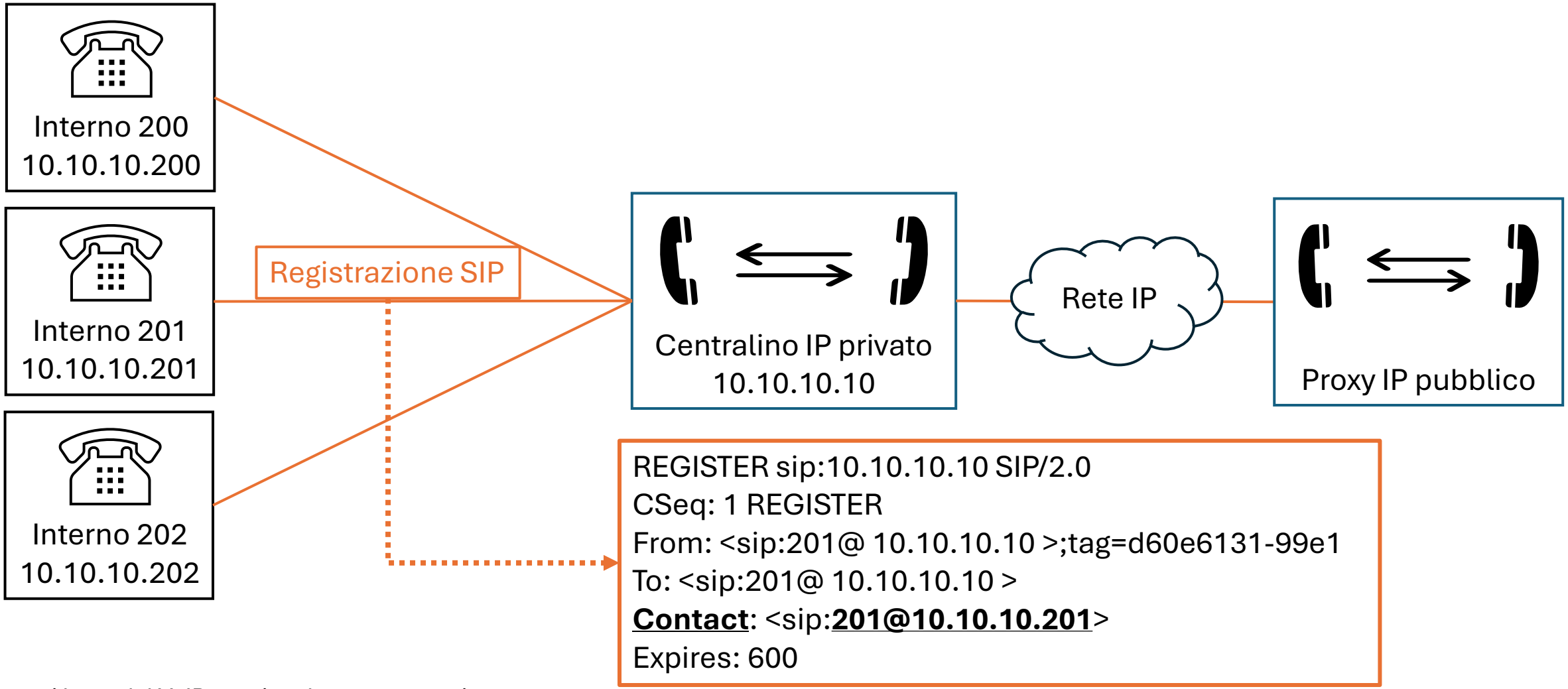
L’evoluzione ci porta all’inversione dei ruoli



I concetti base del VoIP, un piccolo passo avanti.

Telefonia VoIP

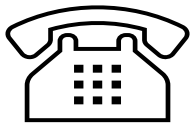
Interazione tra telefoni e centralino



I concetti base del VoIP, un piccolo passo avanti.

Telefonia VoIP

I primi problemi... REGISTER Hijacking



Interno 201
10.10.10.201

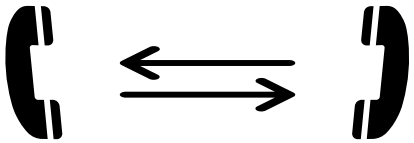
Malintenzionato
10.10.10.150

Registrazione SIP legittima
sip:201@10.10.10.201

Cancellazione della registrazione SIP legittima
sip:201@10.10.10.201

```
REGISTER sip:10.10.10.10 SIP/2.0
From: <sip:201@ 10.10.10.10 >;tag=d60e6131-77da
To: <sip:201@ 10.10.10.10 >
Contact: *
Expires: 0
```

Creazione della registrazione SIP malevola
sip:201@10.10.10.150



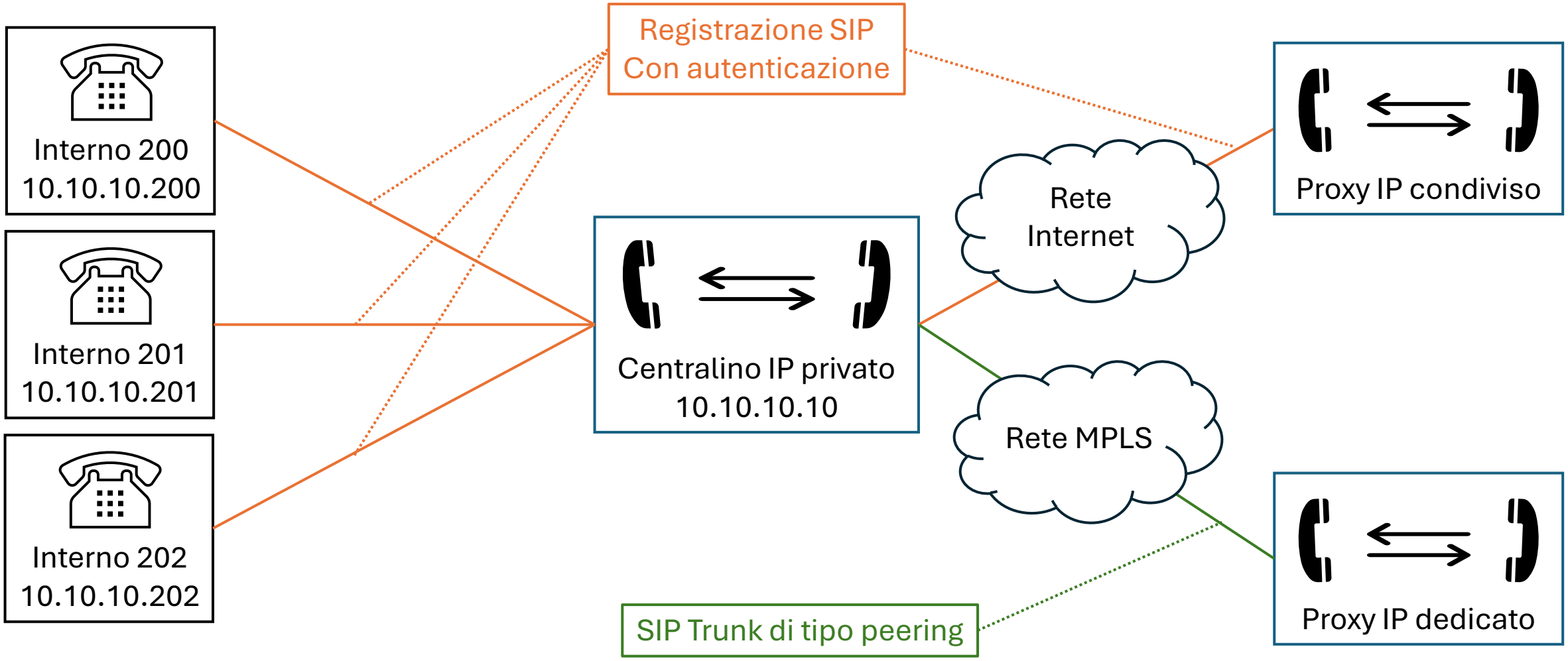
Centralino IP
10.10.10.10

I concetti base del VoIP, un piccolo passo avanti.

Implementazione minimal: quali rischi si corrono?

Telefonia VoIP

Interazione tra telefoni e centralino

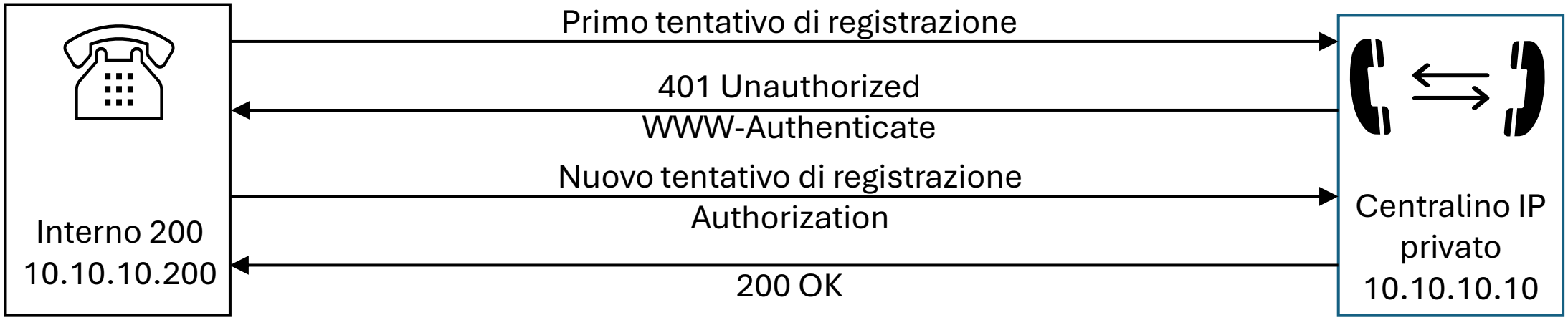


Implementazione minimal: quali rischi si corrono?

Telefonia VoIP

Autenticazione SIP

- Processi di autenticazione molto simili all'HTTP;
- Agli albori era prevista la basic authentication, ad oggi deprecata;
- Utilizzata sia per la ricezione di chiamate in ingresso, che per effettuare chiamate in uscita.



Implementazione minimal: quali rischi si corrono?

Telefonia VoIP

Autenticazione SIP

- Digest composto da elementi statici e dinamici

WWW-Authenticate header (generato dal server)
Digest realm="ExampleRealm", nonce="RandomeNonce", algorithm=MD5, qop="auth"

Password (condivisa preventivamente)
ExamplePassword

Step 1
ha1 = md5(username:realm:password)

Step 2
ha2 = md5(method:uri)

Step 3
digest = md5(ha1:nonce:nc:cnonce:qop:ha2)

Authorization header (generato dal client)
Digest username="ExampleUserName", realm="ExampleRealm", nc=00000001, nonce="RandomeNonce", cnonce="Default_Cnonce", uri="sip:destuser@destdomain.it", qop=auth, algorithm=MD5, response="4006144518ebc3ffbca 597643eadfad6"

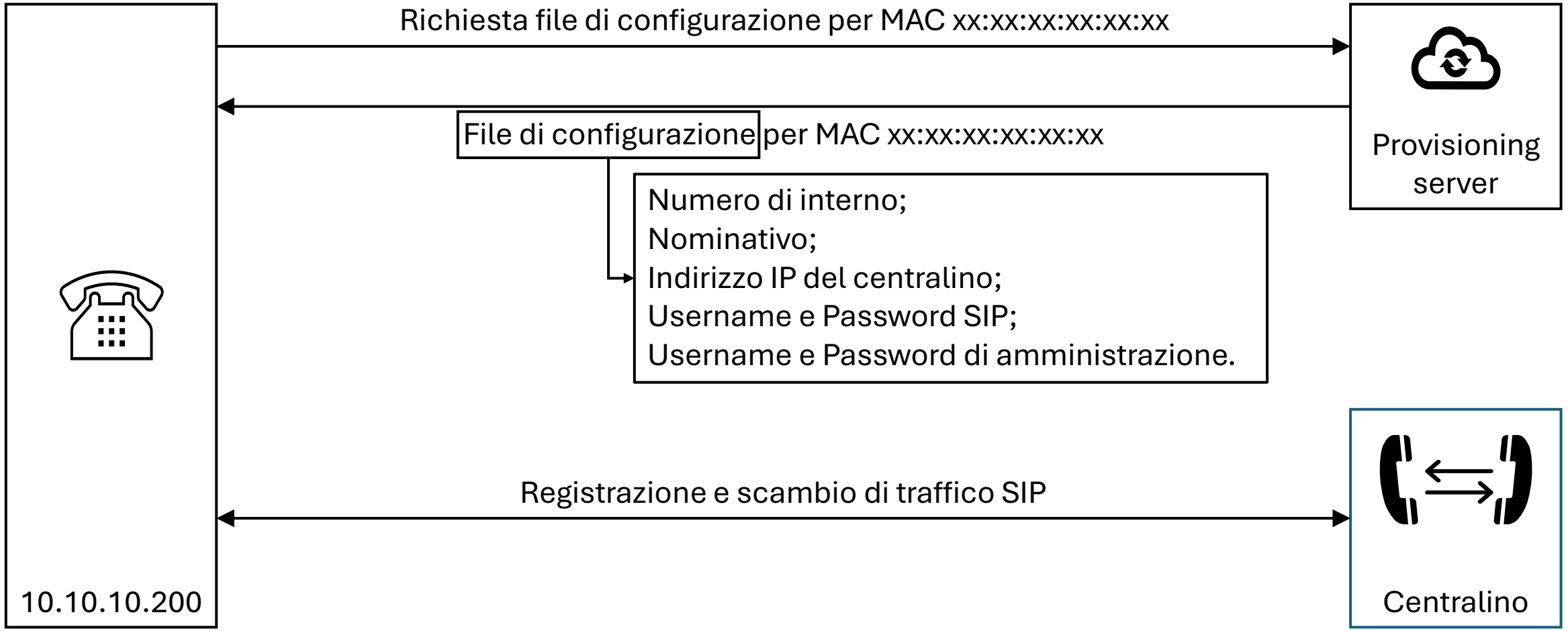
Problema: il processo di autenticazione è debole

Implementazione minimal: quali rischi si corrono?

Telefonia VoIP

Provisioning dei terminali

- Nei sistemi con molti terminali si ricorre al provisioning centralizzato.

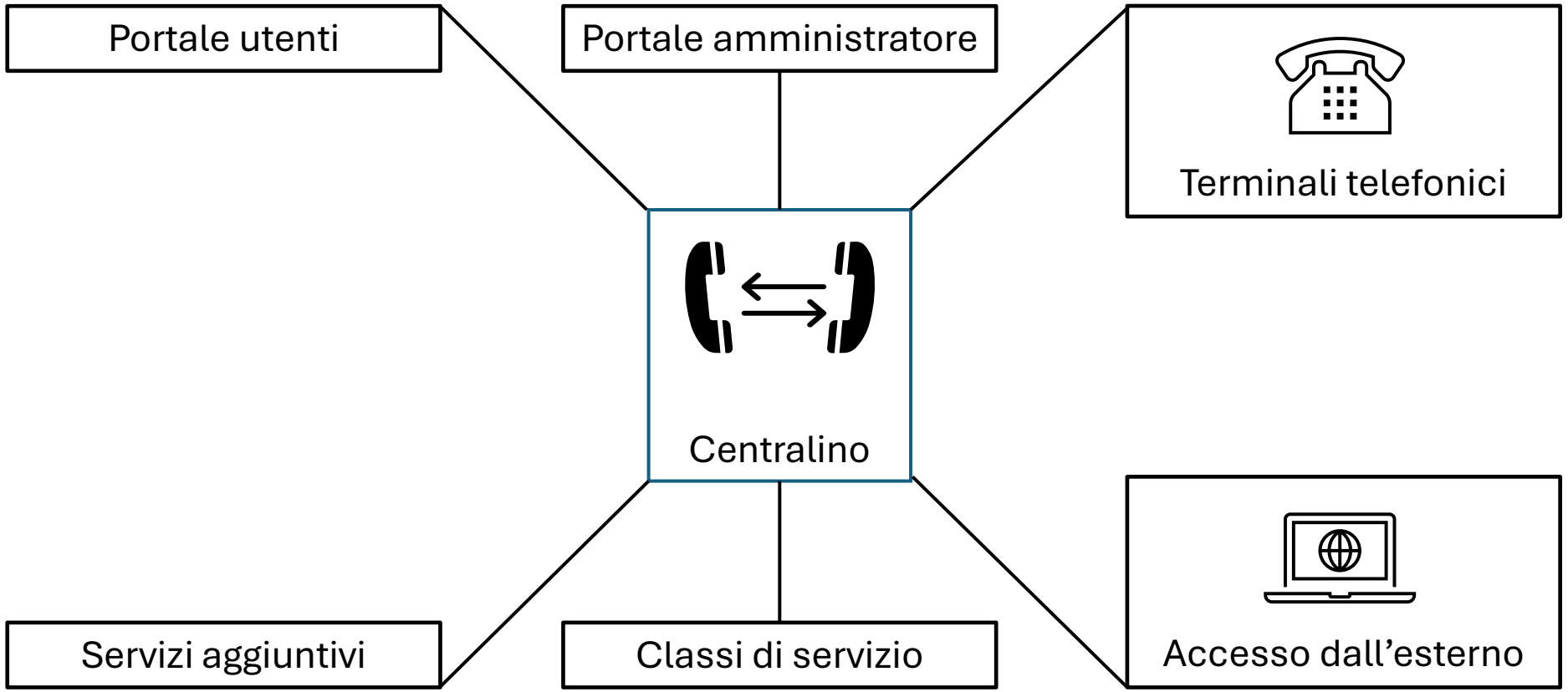


Implementazione minimal: quali rischi si corrono?

Telefonia VoIP

Altri punti di attenzione

- Erogazione dei servizi di centralino tramite interfaccia web o interfaccia vocale;
- Adeguata protezione dei terminali.

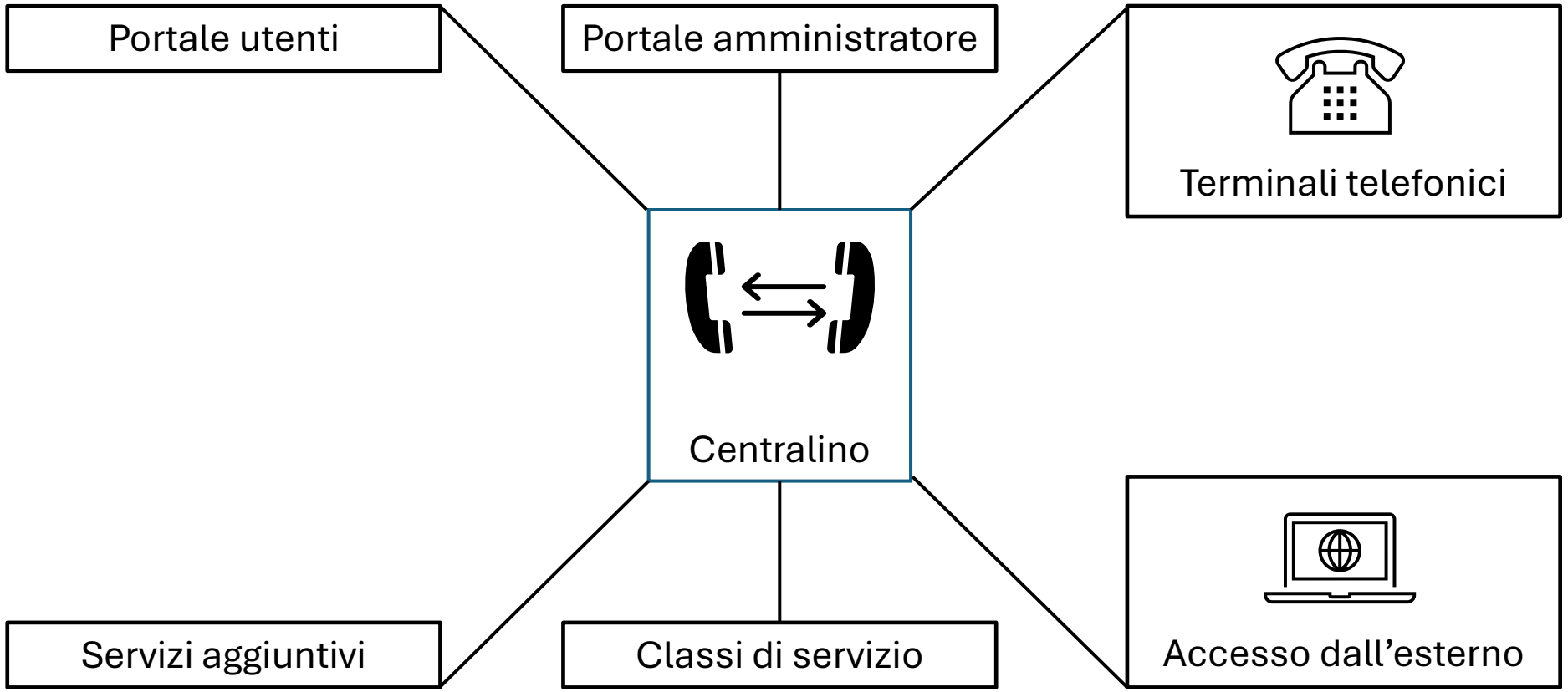


Implementazione minimal: quali rischi si corrono?

Telefonia VoIP

Primi ma fondamentali step

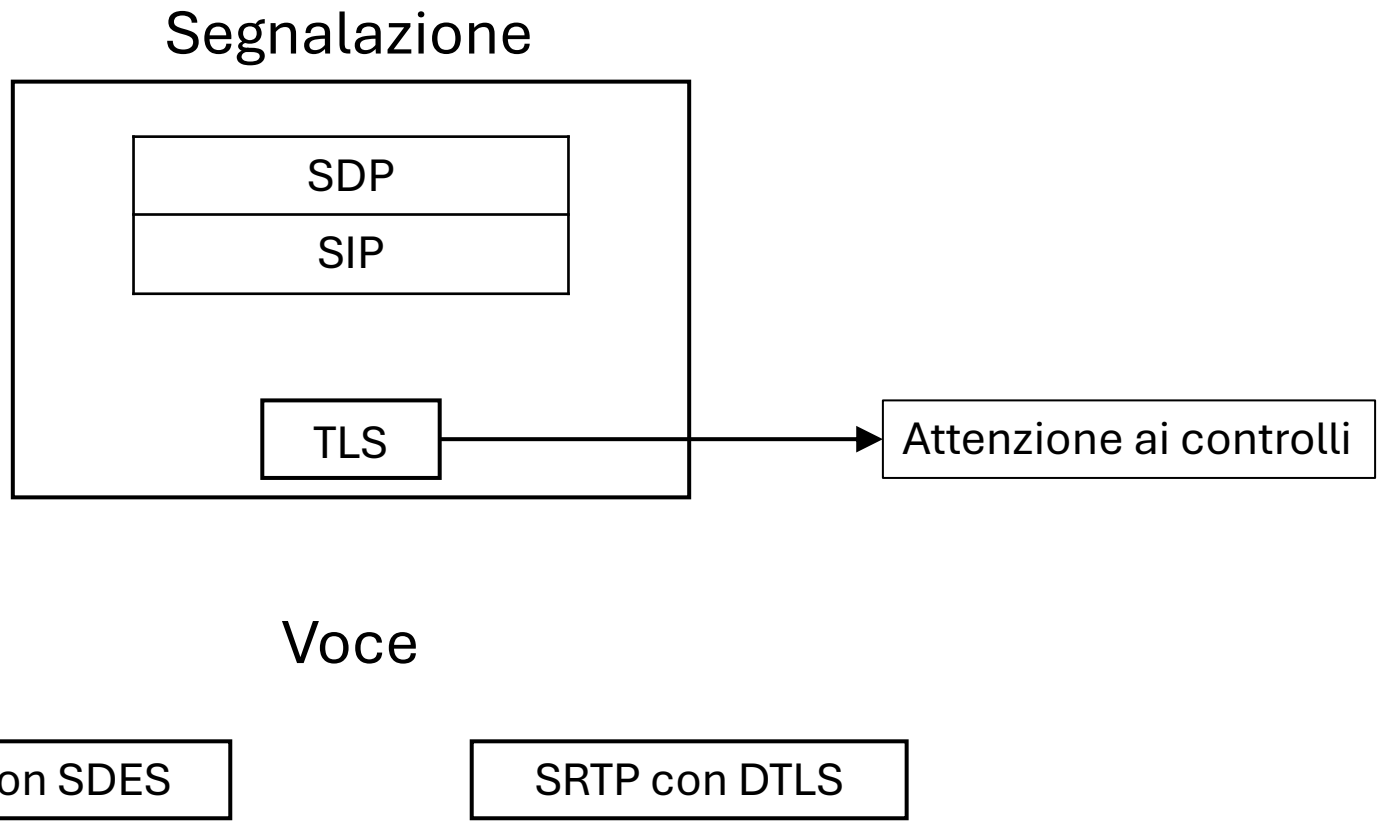
- Avere contezza completa del sistema telefonico attivo;
- Verificare vulnerabilità e relative mitigazioni di tutti i componenti.



Mettere in sicurezza il proprio sistema telefonico.

Telefonia VoIP

L’evoluzione dei protocolli VoIP per migliorare la sicurezza



Mettere in sicurezza il proprio sistema telefonico.

Telefonia VoIP

SDES vs DTLS

SRTP con SDES

```
m=audio 3479 RTP/SAVP 18 8 101
a=rtcp:3480
a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:ExampleKey1|2^31
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:ExampleKey2|2^31
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:ExampleKey3|2^31|1:1
a=rtpmap:18 G729/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
```

SRTP con DTLS

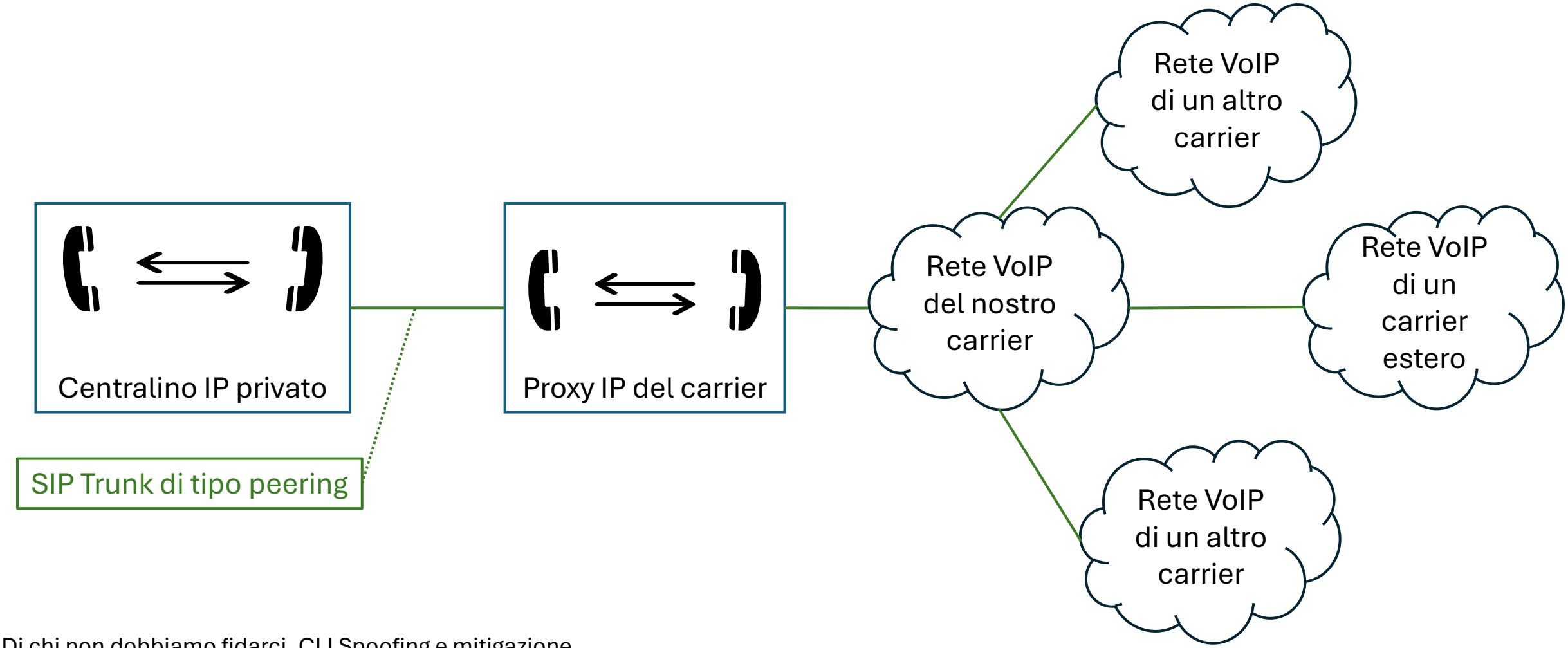
```
m=audio 3479 RTP/SAVP 18 8 101
a=rtcp:3480
a=setup:actpass
a=fingerprint: SHA-1\4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
a=rtpmap:18 G729/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
```

Mettere in sicurezza il proprio sistema telefonico.

Telefonia VoIP

Ma chi garantisce l'identità del chiamante

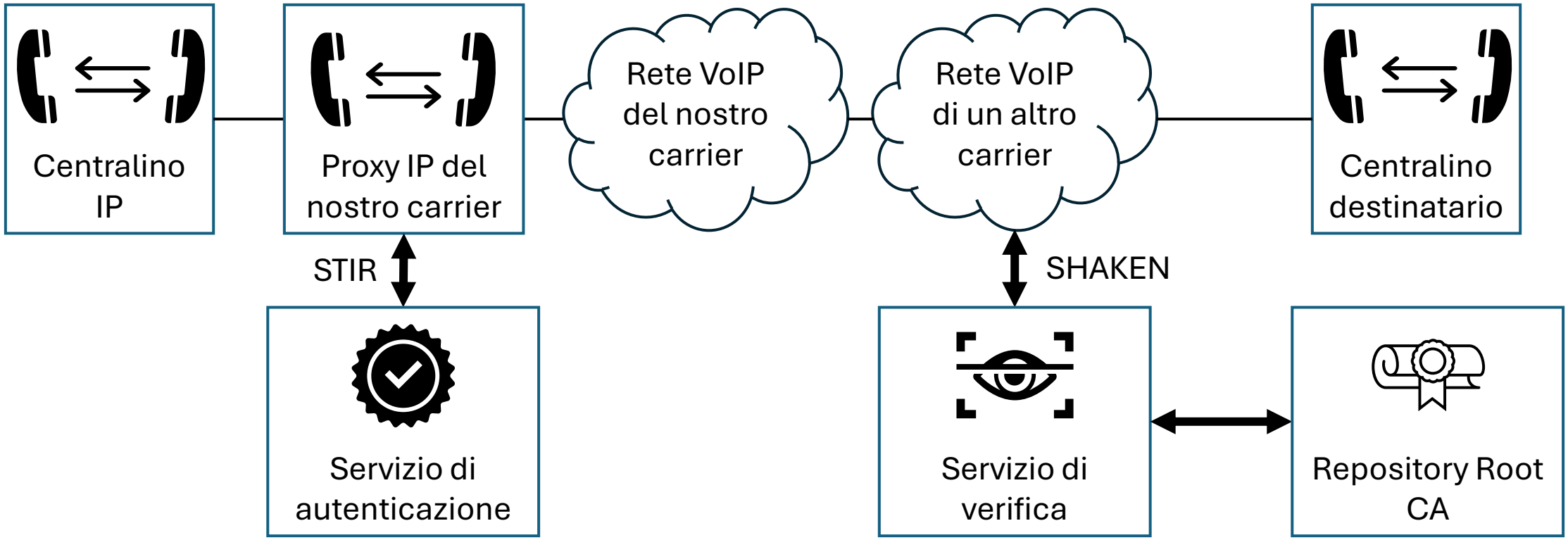
La messa in sicurezza del sistema telefonico non garantisce al 100% la sicurezza del servizio telefonico.
Alcuni elementi è obbligatorio delegarli all'esterno, tra cui la verifica dell'ID Chiamante (CLI).



Di chi non dobbiamo fidarci. CLI Spoofing e mitigazione.

Telefonia VoIP

Una soluzione tecnica: STIR / SHAKEN



Telefonia VoIP

La firma digitale nelle telefonate

Identity SIP Header

```
{
        "alg": "ES256",
        "ppt": "shaken",
        "typ": "passport",
        "x5u": "https://cert.esempio.it/HiB.pem"
}
{
        "attest": "A",
        "dest": {
                "tn": [
                        “DestPhoneNumber"
                ]
        },
        "iat": 1762293829,
        "orig": {
                "tn": " SRCPhoneNumber "
        },
        "origid": “jjjjjjjj-xxxx-dddd-ffff-iiiiiiii"
}
```

Livello di attestazione	Descrizione
A	Attestazione completa (chiamante + numero)
B	Attestazione parziale (solo chiamante)
C	Attestazione di tipo gateway (niente)

Firmato digitalmente dal carrier originante

Telefonia VoIP

Conclusioni

- L’autorizzazione all’utilizzo del numero di telefono non implica il possedimento dello stesso, molto difficilmente sapremo chi utilizza il nostro numero telefonico e per quali scopi;
- La sicurezza del nostro sistema telefonico, insieme ai protocolli implementati dai carrier aiuta a diminuire gli utilizzi non autorizzati delle nostre numerazioni;
- La sicurezza della nostra identità telefonica dipende sia da noi, che dalla rete globale, su certi aspetti non possiamo farci niente.
- In futuro ci sarà una svolta? Forse

VoIP: hands-on protocol