

# Indelli Videoconferenza SFU

---

## Specifiche Tecniche del Sistema:

### "Indelli Videoconferenza SFU & Loquimini Chat"

**Architettura WebRTC, Selective Forwarding Unit (Mediasoup), Integrazione Frame e Privacy-by-Design**

## 1. Introduzione e Obiettivi Architetturali

Il sistema "Indelli Videoconferenza SFU" rappresenta una soluzione di comunicazione unificata progettata per garantire flussi audio/video stabili e sicuri. Basato su architettura WebRTC SFU (Selective Forwarding Unit) tramite il motore Node.js 'Mediasoup', il sistema è progettato per ottimizzare l'uso della banda e scalare orizzontalmente. La peculiarità dell'architettura è l'incapsulamento a frame, che integra nativamente il modulo di chat effimera multilingua 'Loquimini', offrendo un ecosistema di comunicazione istituzionale completo.

## 2. Architettura Server (SFU) e Ottimizzazione Hardware

Il server di signaling e di instradamento multimediale è scritto in Node.js (ECMAScript Modules) e implementa logiche di ottimizzazione hardware estreme:

- - Multi-Worker e CPU Affinity (Pinning): Il sistema avvia un pool di worker Mediasoup (es. 8 worker). Cruciale per architetture asimmetriche (come Ryzen 9 9950X3D), il server esegue il 'pinning' di ogni worker esclusivamente sui core fisici pari (0, 2, 4...), massimizzando l'efficienza della cache ed evitando i colli di bottiglia dell'Hyper-Threading.
- - Load Balancing Interno (Round-Robin): Le nuove stanze virtuali (Rooms) vengono distribuite ciclicamente tra i worker fisici disponibili, bilanciando il carico computazionale della cifratura/decifratura RTP.
- - Signaling via WebSocket e TURN Server: Il server gestisce il signaling su porta dedicata (55008) e genera dinamicamente le credenziali crittografiche temporanee (HMAC-SHA1) per il server TURN/STUN, essenziale per attraversare NAT e Firewall aziendali complessi.
- - Codec Ottimizzati: Il traffico multimediale è ristretto a Opus (Audio 48kHz stereo) e VP8 (Video 90kHz), garantendo massima compatibilità cross-browser e basso footprint.

### 3. Architettura Client e Resilienza di Rete

Il client (sviluppato in JavaScript vanilla interfacciato con mediasoup-client) gestisce la logica di acquisizione e riproduzione in modo reattivo:

- - Reconnection Strategy (Grace Period): In caso di disconnessione (es. caduta del Wi-Fi), il client implementa un delay esponenziale (fino a 10s) per tentare la riconnessione al WebSocket. Il server, a sua volta, concede un 'grace period' di 5 secondi prima di effettuare il cleanup definitivo del peer, evitando chiusure accidentali.
- - Consume & Produce Pattern: Il client istanzia due trasporti WebRTC separati (uno per l'invio - sendTransport, uno per la ricezione - recvTransport), garantendo un controllo granulare sulle tracce audio/video e permettendo mute/unmute lato client senza abbattere la connessione.
- - Auto-Grid e DOM Manipulation: La UI si adatta dinamicamente inserendo o rimuovendo i tag <video> in tempo reale (gestendo workaround specifici per browser desktop, come il mute temporaneo per evitare black screen) e aggiornando il CSS Grid layout (1x1, 2x2, 3x3) in base al numero di partecipanti.

### 4. Integrazione Loquimini e Ingressi

Il modulo video non lavora in isolamento. Attraverso l'uso di iframe (sistema a Frame), la videoconferenza viene affiancata alla chat istituzionale 'Loquimini'.

Il flusso di ingresso (pre-stanza) è gestito da script PHP (come partecipanti.php) che raccolgono le variabili di sessione, la lingua selezionata e l'identificativo della stanza. Questo assicura che gli utenti (cittadini o funzionari) accedano a un ambiente unificato dove la comunicazione verbale (SFU) si sposa con la traduzione testuale multilingua asincrona fornita dal modulo Loquimini.

### 5. Matrice Privacy-by-Design e Confronto con Soluzioni Commerciali

Nell'ambito della Pubblica Amministrazione, l'adozione di soluzioni di videoconferenza commerciali (es. Zoom, Microsoft Teams, Google Meet) espone gli Enti a criticità normative (GDPR) e di data sovereignty. Il sistema Indelli affronta e risolve questi rischi strutturali grazie al suo approccio On-Premise e Privacy-by-Design:

| <b>Dimensione Privacy / Sicurezza</b>  | <b>Soluzioni Commerciali (Zoom, Teams, Meet)</b>                                                                  | <b>Indelli Videoconferenza SFU (On-Premise)</b>                                                                                       |
|----------------------------------------|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Sovranità dei Dati (Data Sovereignty)  | Il traffico audio/video transita su server esteri (spesso extra-UE), soggetti a normative estere (es. Cloud Act). | Traffico gestito internamente. Nessun byte esce dall'infrastruttura di rete della Pubblica Amministrazione.                           |
| Ritenzione Dati e Metadati (Telemetry) | Registrazione estensiva di metadati (durata, IP, dispositivi, log di chat) a scopi di profilazione e analytics.   | Zero telemetria. Nessun tracciamento comportamentale o archiviazione occulta dei metadati degli utenti.                               |
| Effimerità (Ephemerality)              | Chat e file condivisi spesso persistono nei cloud provider dopo la chiusura della chiamata.                       | Integrazione con Loquimini: le sessioni sono strettamente volatili. Alla chiusura, cartelle e dati vengono distrutti automaticamente. |
| Vendor Lock-in e Dipendenza            | Infrastrutture chiuse. Necessità di installare client pesanti o dipendenza da licenze SaaS rinnovabili.           | Sistema open-core basato su standard WebRTC aperti (no-plugin, no-install). Accesso diretto via browser web standard.                 |

Il trasporto multimediale avviene attraverso crittografia end-to-end standard WebRTC (DTLS-SRTP). Poiché il server SFU è ospitato direttamente nei datacenter dell'Ente, la decifratura e il re-instradamento dei pacchetti non comportano mai l'esposizione dei flussi a entità terze, garantendo la totale rispondenza ai vincoli del Garante Privacy.