

Specifiche Tecniche del Sistema:

Architettura di Sorveglianza Urbana Decentralizzata & SFU Streaming

Infrastruttura WebRTC Edge-First, Debian 13, Crittografia LUKS, Medie Mobili e Privacy-by-Design

1. Introduzione e Obiettivi Architettureali

Il sistema di videosorveglianza e streaming urbano rappresenta una soluzione tecnologica avanzata, progettata per garantire flussi video ad altissima stabilità, totale sovranità del dato e conformità rigorosa alle normative europee (GDPR e EU AI Act). Svincolandosi dai costosi "black box" proprietari, l'architettura adotta un paradigma decentralizzato edge-first, basato su nodi periferici autonomi e flussi da dispositivi mobili, interconnessi a una sala operativa centrale tramite standard WebRTC e il motore Selective Forwarding Unit (SFU) Mediasoup.

2. Architettura Server Centrale e Ottimizzazione Hardware

Il nodo centrale gestisce lo smistamento dei flussi video in tempo reale e l'inferenza di intelligenza artificiale forense:

- **Core di Comunicazione SFU:** Sviluppato su stack Node.js, utilizza Mediasoup per l'instradamento efficiente dei pacchetti multimediali senza onerose ricodifiche, riducendo drasticamente il carico computazionale.
- **Potenza di Calcolo e Analisi On-Premise:** Postazione centrale dotata di hardware multi-core e GPU dedicate (es. RTX serie 50) per l'elaborazione locale dei fotogrammi in caso di emergenza o indagini giudiziarie.
- **Segnalazione e Trasporto:** Gestione dei flussi protetta da standard WebRTC (DTLS-SRTP), garantendo comunicazioni cifrate end-to-end senza esposizione a server o cloud di terze parti.

3. Architettura delle Postazioni Fisse (I Nodi Periferici)

Le postazioni fisse sul territorio (installate su pali o punti sensibili) operano in totale autonomia:

- **Sistema Operativo e Gestione:** Debian 13 con ambiente grafico XFCE, amministrato in remoto via XRDP con indirizzo IP dedicato.
- **Resilienza e Avvio Automatico:** Configurazione tramite servizi systemd per garantire il ripristino automatico e immediato dei flussi di streaming (tramite browser Firefox in modalità kiosk) e dei processi di registrazione a ogni boot.
- **Doppio Storage e 'Scatola Nera' Locale:**
 - **SSD Primario:** Dedicato al sistema operativo e servizi in chiaro, per garantire riavvio e connessione XRDP immediata.
 - **SSD Secondario (o Box Esterno Blindato):** Dedicato alle registrazioni (15 giorni, 500GB) con sovrascrittura ciclica.

4. Integrazione Tattica su Medie Mobili (Smartphone/Tablet)

Oltre ai nodi fissi, l'infrastruttura si estende nativamente e senza attriti a operatori in campo e unità mobili (pattuglie), trasformandosi in un vero ecosistema ibrido C4ISR:

- **Accesso via Link Web (Zero-Install):** Grazie all'architettura WebRTC standard, l'operatore non deve installare app proprietarie (no SDK blindati). È sufficiente aprire un URL (banale link di stanza virtuale) dal browser dello smartphone (Safari/Chrome).
- **Trasmissione Live dal Campo:** Lo smartphone diventa istantaneamente una telecamera mobile connessa alla sala operativa, sfruttando la rete cellulare. Il server SFU gestisce la ricezione adattiva del flusso video.
- **Condivisione Multi-Dispositivo:** Le medie mobili si integrano alla perfezione nel layout a griglia del sistema centrale, affiancando i feed delle postazioni fisse, permettendo al centro di controllo di avere occhi sia sulle postazioni permanenti che sul personale dispiegato in emergenza.

5. Sicurezza Fisica e Crittografia a Riposo (LUKS)

Sulle postazioni fisse, per soddisfare i massimi standard di sicurezza e protezione dei dati:

- **Blindatura Crittografica (LUKS):** Il secondo SSD contenente le videoregistrazioni storiche è interamente cifrato.
- **Zero-Key Persistence e Accesso Forense:** Nessuna chiave di sblocco risiede sul disco. L'accesso ai video richiede l'intervento remoto di un operatore via XRDP che decifra il volume esclusivamente per le operazioni di esportazione autorizzata.

6. Matrice di Conformità: Privacy-by-Design vs Soluzioni Commerciali

Dimensione Privacy / Sicurezza	Soluzioni Commerciali / Cloud	Architettura Urbana Decentralizzata
Sovranità dei Dati (Data Sovereignty)	Il traffico video transita su server esteri (extra-UE), esposto a normative di terze parti.	Traffico confinato interamente nell'infrastruttura locale dell'Ente. Nessun byte esce dal perimetro di controllo.
Tracciamento e Telemetria	Raccolta estensiva di metadati e log a fini di profilazione.	Zero telemetria. Nessuna app mobile proprietaria richiesta, traffico diretto su browser.
Gestione dello Storico ('Scatola Nera')	Persistenza indefinita dei dati su cloud proprietari non verificabili.	Registrazione locale autonoma di 15 giorni su disco cifrato LUKS (fissi) + flussi mobili volatili e diretti.
Accessibilità Mobile	Vincolata all'installazione di App (MDM) e licenze per singolo operatore.	Standard WebRTC aperto. Accesso tattico via browser smartphone con un semplice link.