2.1 *Dati di dimensionamento e tempi di risposta (latency)*

In seguito alla raccolta delle informazioni di traffico fornite dalle Forze di Polizia (Arma dei Carabinieri e Polizia di Stato) è stato stimato in circa 20, il numero complessivo massimo delle chiamate di emergenza (112, 113) simultanee. Di conseguenza, si può ritenere in 20 rloc/sec [6], anche il numero complessivo massimo delle richieste di localizzazione simultanee.

Tale valore dovrà essere ripartito fra tutti gli Operatori di Telefonia (fissa e mobile).

Per quanto riguarda la provenienza delle chiamate di emergenza — dalla rete mobile o dalla rete fissa — i dati di traffico degli Operatori di Telefonia indicano nel valore del 90% la percentuale delle chiamate di emergenza dalla rete mobile e nel 10% quelle dalla rete fissa.

In merito ai tempi di risposta (latency), la localizzazione del «chiamante» - a seguito della richiesta iniziata dai PSAP (CO 112/113) - deve essere del tipo che possa essere soddisfatta in maniera rapida.

Si richiede quindi che i sistemi informatici di ciascun Operatore di Telefonia — con la chiamata di emergenza in corso — rendano disponibile l'informazione di localizzazione — *nelle condizioni di massimo carico* [7] — approssimativamente entro 4 secondi, a partire dalla ricezione della richiesta di localizzazione proveniente dal CED Interforze [8]. L'intervallo in questione sarà individuato a partire dalla ricezione della richiesta di localizzazione in capo al Gateway dell'Operatore che ha in carico l'utente chiamante e fino all'invio della risposta dallo stesso gateway.

2.2 *Interconnessione CED Interforze - PSAP (CO 112/113)*

Attualmente, per l'Arma dei Carabinieri e la Polizia di Stato sono già presenti i collegamenti per l'interconnessione al CED Interforze, rispettivamente tramite CDN e la c.d. «multimediale» (**Figura 2**).

Nell'architettura di rete, relativa all'interconnessione tra i PSAP (CO 112/113) presenti sul territorio nazionale e il «concentratore interforze», presso il CED Interforze sarà prevista una capacità di banda complessiva (massima) di circa 10 Mbit/sec.

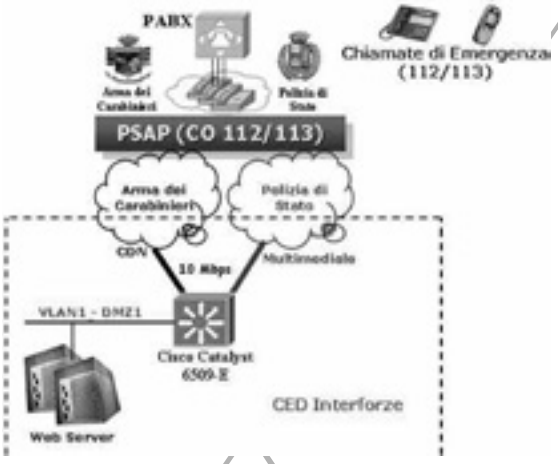

Figura 2 - *Interconnessione CED Interforze - PSAP (CO 112/113)*

Gli standard di sicurezza della comunicazione per il livello applicativo (layer 7) saranno assicurati mediante l'adozione del protocollo HTTPS (HTTP con protocollo sicuro SSL v3). L'autenticazione al livello applicativo avverrà tramite una mutua autenticazione tra il «concentratore interforze» e il generico PSAP (CO 112/113) mediante lo scambio di certificati digitali [9].

L'ente di certificazione (CA) preposto al rilascio dei certificati digitali per la mutua autenticazione (HTTPS) sarà il CED Interforze del Ministero dell'Interno.

2.3 *Interconnessione CED Interforze - Operatori di Telefonia*

Per l'interconnessione tra il «concentratore interforze» (CED Interforze) e ciascun Operatore di Telefonia, sarà implementata una VPN (Virtual Private Network). Ogni VPN, permetterà di stabilire un canale di comunicazione «sicuro» creando un «tunnel IPSec» site-to-site [10] (**Figura 3**).

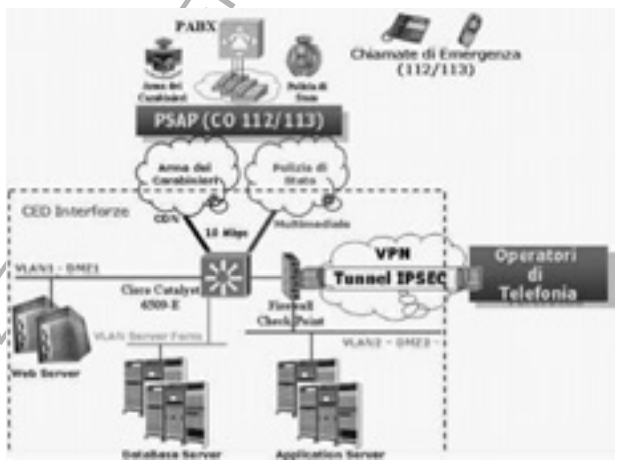

Figura 3 - *Interconnessione CED Interforze - Operatori di Telefonia*

Il collegamento VPN IPSec - lato CED Interforze - sarà implementato tramite un Firewall Check Point (piattaforma software Check Point NGX). Tale piattaforma sarà in grado di gestire almeno 200 connessioni simultanee VPN IPSec [11].

Tra gli apparati gateway rispettivamente del CED Interforze (Firewall Check Point) e del generico Operatore di Telefonia, sarà implementata una VPN con protocollo di comunicazione IPSec, che utilizzerà gli algoritmi: *AES con chiave di lunghezza 256 bit e SHA-1*.

Tali apparati gateway dovranno essere raggiungibili tramite indirizzi IP pubblici. Il CED Interforze e ciascun Operatore di Telefonia dovranno inoltre, definire e concordare i rispettivi piani di indirizzamento IP in modo tale da garantire la *raggiungibilità* delle rispettive «componenti» dei sistemi informatici che forniranno il servizio di localizzazione.

L'autenticazione degli estremi del «tunnel IPSec» avverrà tramite l'utilizzo di certificati digitali X.509 v3, rilasciati da una Certification Authority (CA).

---

[6] Il valore comprende le richieste di localizzazione sia a seguito delle chiamate di emergenza, sia a seguito delle richiamate di emergenza.

[7] Ossia del numero massimo di richieste di localizzazione previste per ciascun Operatore di Telefonia.

[8] Tale requisito risponde ai desiderata delle Amministrazioni che gestiscono le emergenze, che possono in questo modo usare questa informazione rapida a supporto delle decisioni senza ritardi nella gestione della chiamata. Secondo quanto riportato nel Rapporto del CGALIES «... initial position should be available approximately 7 seconds after the call is initiated. In general, the emergency services requirements on latency are that an approximate position (Cell ID is sufficient) is available in ~15 seconds».

[9] HTTPS con mutua autenticazione.

[10] Una rete virtuale privata «sicura» (SVPN) è costituita da un insieme di nodi collegati tra loro attraverso una rete geografica, generalmente pubblica (ad esempio: Internet), in modo tale da realizzare una rete privata «simulando» il comportamento di link geografici dedicati. Quindi, l'utilizzo di una rete privata virtuale permette di stabilire dei collegamenti a livello di infrastruttura della rete e di rendere sicuro il traffico site-to-site, creando un «tunnel» IPSec, ossia il veicolo che incapsula e trasporta le informazioni tra gli end-point.

[11] Si ritiene in 100 il numero stimato degli Operatori di Telefonia da prendere in considerazione.