

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-site¹⁰ (Figura 3).

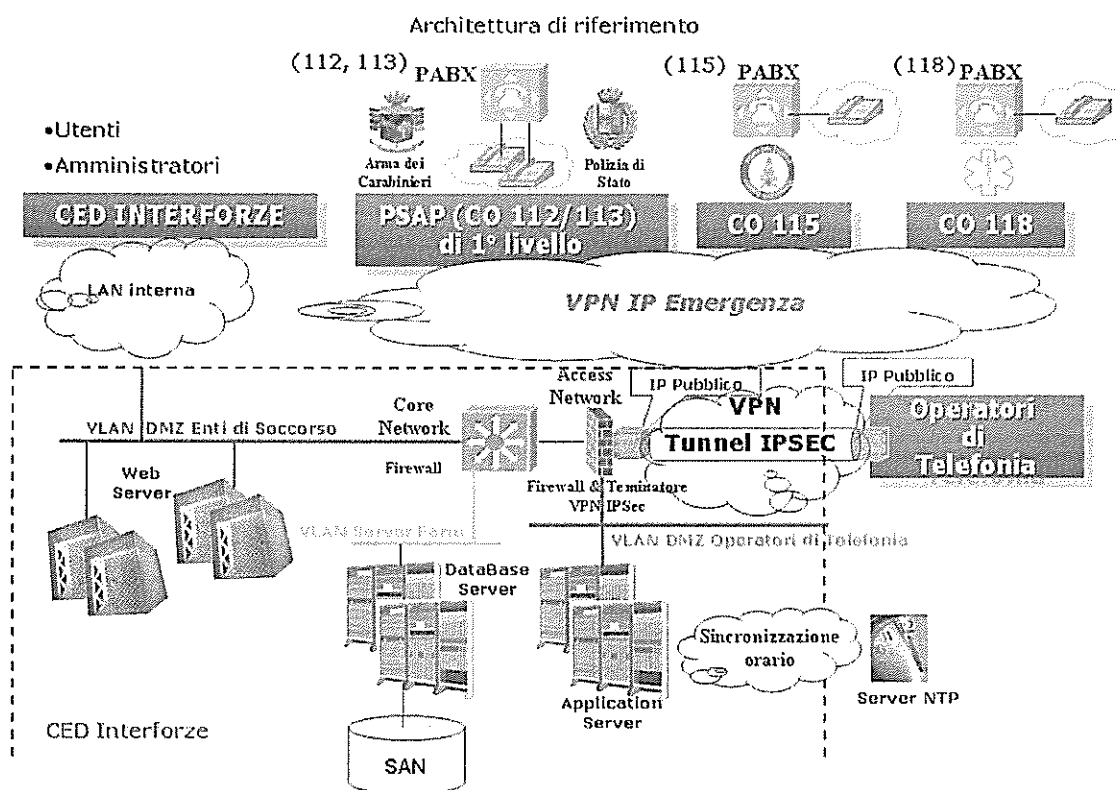
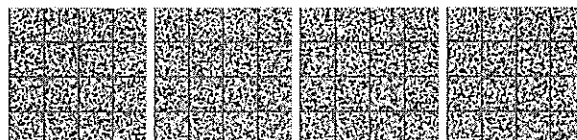


Figura 3 - Interconnessione CED Interforze - Operatori di Telefonia

Il collegamento VPN IPsec - lato CED Interforze - sarà implementato tramite una piattaforma tecnologica Firewall/Terminatore VPN. Tale piattaforma sarà in grado di gestire almeno 200 connessioni simultanee VPN IPsec¹¹.

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.



Tra gli apparati gateway rispettivamente del CED Interforze 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).

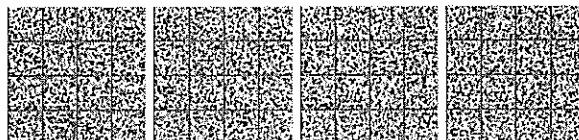
L'ente di certificazione (CA) preposto al rilascio dei certificati digitali per l'autenticazione degli estremi del “tunnel IPSec” (VPN) sarà il CED Interforze del Ministero dell'Interno.

La sicurezza della comunicazione sarà garantita tramite l'adozione della suite di protocolli IPSec (Internet Protocol Security) per livello di rete (layer 3), mentre per il livello applicativo (layer 7) gli standard di sicurezza saranno assicurati mediante l'adozione del protocollo HTTPS (HTTP con protocollo sicuro SSL v3). In particolare per il protocollo HTTPS dovrà essere abilitata la porta 10036.

L'autenticazione al livello applicativo avverrà attraverso UserID e Password, il “concentratore interforze” richiederà il servizio di localizzazione utilizzando l'HTTP POST request e la risposta sarà inviata attraverso l'HTTP response.

In alternativa potrà essere gestita una mutua autenticazione tra Client (CED Interforze) e Server (Operatore di Telefonia) mediante scambio di certificati digitali¹¹. L'ente di certificazione (CA) preposto al rilascio dei certificati digitali per la mutua autenticazione (HTTPS) sarà il CED Interforze del Ministero dell'Interno.

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



Nell'ambito dell'interconnessione tra il CED Interforze e gli Operatori di Telefonia - per il progetto NUE integrato - la Figura 4 che segue illustra l'architettura generale di rete per l'accesso alla rete Internet da parte del CED Interforze.

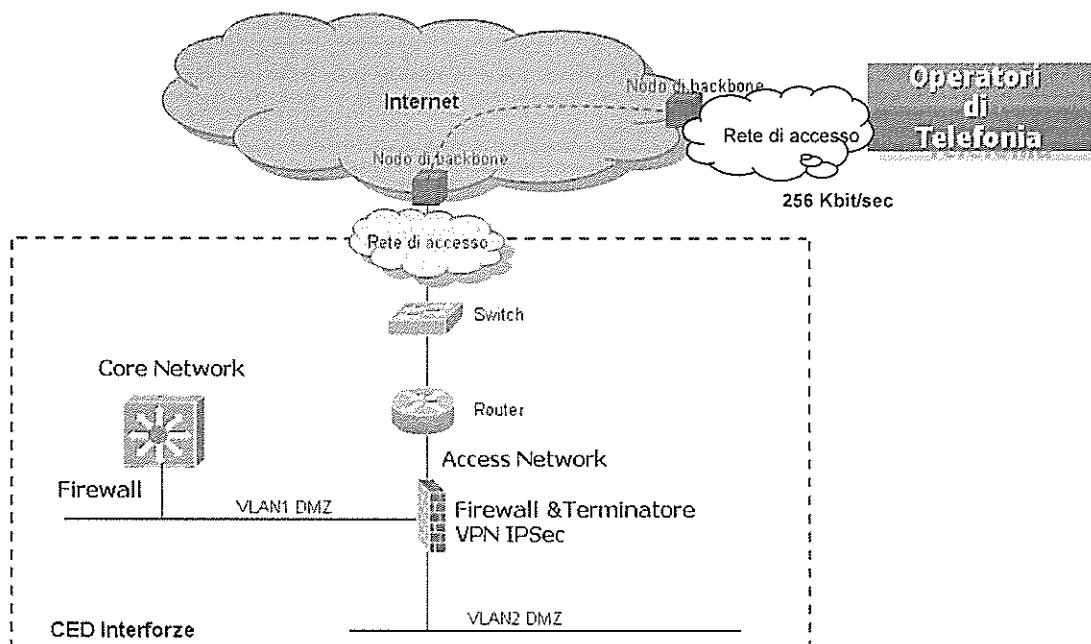


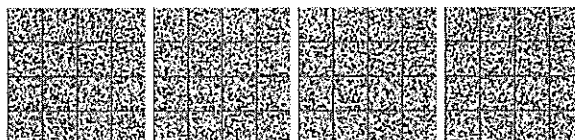
Figura 4 - Architettura di rete per l'accesso alla rete pubblica

Per quanto riguarda la capacità del canale di trasporto delle informazioni, considerando una dimensione massima per i messaggi ELIR o ELIA di circa 2 Kbyte, i dati di traffico in precedenza esposti ed infine l'overhead introdotto dal solo protocollo IPSec (circa il 20 %), si richiede agli Operatori di Telefonia (sulla propria rete di accesso) una banda minima garantita di 256 kbit/sec. In virtù dei requisiti del Servizio Numero Unico Europeo per le Emergenze, l'infrastruttura tecnologica dovrà essere ad alta affidabilità.

Di conseguenza, nelle soluzioni architetturelle previste a livello di PSAP di 1° livello, Sale/Centrali Operative CO 115 e CO 118, CED Interforze ed infine Operatori di Telefonia non dovranno essere presenti single-point-of-failure. Quindi, per l'alta affidabilità sarà necessaria la ridondanza nell'hardware previsto per i diversi "layer" dell'infrastruttura tecnologica¹³.

¹² HTTPS con mutua autenticazione.

¹³ Ad esempio ambienti di "cluster" per Application & Database Server o ambienti di "load balancing" per Web Server (front-end).



Visto il requisito che prevede l'alta affidabilità per i diversi "layer" dell'infrastruttura tecnologica, anche il "Network layer" dovrà prevedere la ridondanza degli apparati di rete e dei link fisici per il collegamento alla rete pubblica o all'interno della rete locale. Infatti, una delle cause più comuni dell'interruzione dell'operatività è rappresentata da un guasto nel collegamento verso la dorsale (nodo di backbone) del "provider" di servizi Internet. Quindi, oltre al "collegamento principale" bisognerà prevedere anche un "collegamento di protezione" (Figura 5).

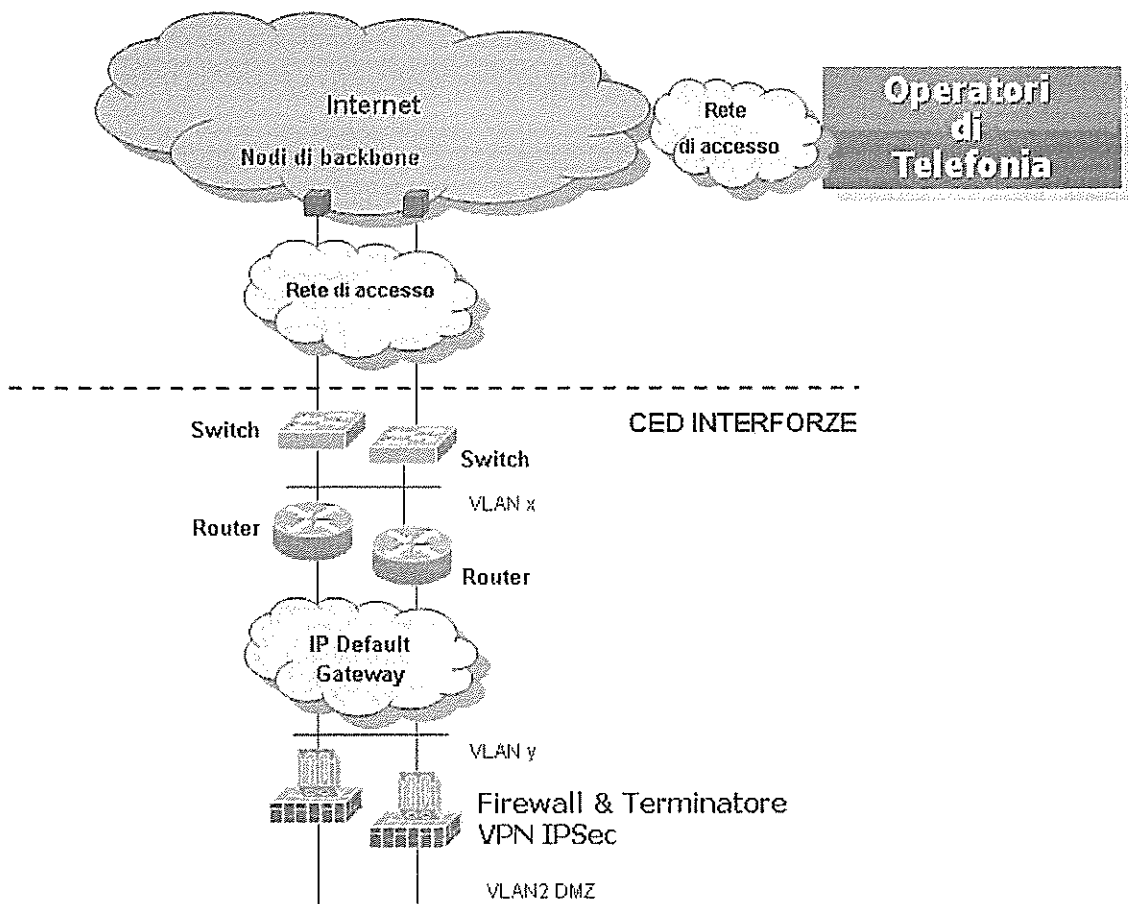
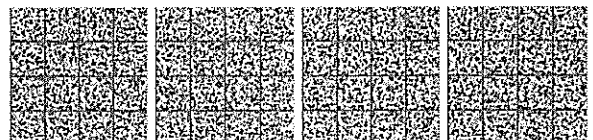


Figura 5 - Architettura di rete ad alta affidabilità per l'accesso alla rete pubblica

Nel caso della ridondanza del router (in configurazione "Active – Standby"), poiché i due apparati di rete avranno "indirizzi" differenti bisognerà prevedere un *meccanismo* (ad esempio: tramite l'adozione di protocolli HSRP, VRRP, ecc...) che utilizzerà un unico "indirizzo" e lo assegnerà sempre all'apparato funzionante.



L'adeguamento ai requisiti generali di interconnessione in precedenza descritti si potrà realizzare secondo un piano da stabilire e concordare, ad esempio per fasi, definendo per ogni fase il livello di adeguamento dell'infrastruttura tecnologica fino ad arrivare alla garanzia del Servizio Numero Unico Europeo per le Emergenze, entro il completamento dell'attivazione del servizio su tutto il territorio nazionale.

ALLEGATO 5

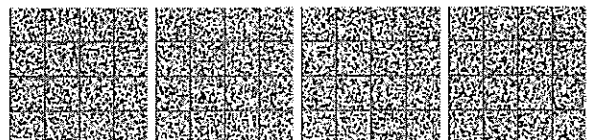
Tempistiche di attivazione del servizio 112NUE

Il servizio, relativamente alle numerazioni di emergenza 112 e 113, sarà attivato nelle province secondo la seguente calendarizzazione:

- Entro il 12 febbraio 2010 18 province
- Entro il 18 marzo 2010 18 province
- Entro il 21 aprile 2010 18 province
- Entro il 26 maggio 2010 18 province
- Entro il 30 giugno 2010 18 province
- Entro il 30 luglio 2010 restanti province

Le province saranno individuate dall'unità per il monitoraggio di cui all'art. 5 del presente decreto, e, comunicate agli operatori entro il 60°/45° giorno antecedente a quello della relativa data di attivazione indicata.

Il presente allegato sostituisce integralmente l'allegato 5 al decreto ministeriale 22 gennaio 2008 citato nelle premesse



Tempistiche di attivazione del servizio 112NUE

Il servizio, relativamente alle numerazioni di emergenza 115 e 118, sarà attivato nelle province secondo la calendarizzazione seguente:

- Entro il 30/07/2010 3 province
- Entro i 12 mesi successivi alla data di completamento delle attività di implementazione delle numerazioni di emergenza 112 e 113 di cui all'allegato 5 del presente decreto, saranno attivate le restanti province.

Le singole province e la relativa tempistica saranno individuate dall'unità per il monitoraggio di cui all'art. 5 del presente decreto, e, comunicate agli operatori entro il 60°/45° giorno antecedente a quello della relativa data di attivazione indicata.

10A01324

DECRETO 16 novembre 2009.

Liquidazione coatta amministrativa della società cooperativa «Dimensione Green Service Società cooperativa», in Massa e nomina del commissario liquidatore.

IL MINISTRO
DELLO SVILUPPO ECONOMICO

Visto il decreto del Presidente della Repubblica 28 novembre 2008, n. 197, recante il regolamento di organizzazione del Ministero dello sviluppo economico, per la parte riguardante le competenze in materia di vigilanza sugli enti cooperativi;

Viste le risultanze della revisione dell'associazione di rappresentanza in data 27 febbraio 2009 dalle quali si rileva lo stato d'insolvenza della società cooperativa sotto indicata:

Viste le risultanze degli ulteriori accertamenti d'ufficio presso il registro delle imprese;

Visto l'art. 2545-terdecies del codice civile e ritenuto di doverne disporre la liquidazione coatta amministrativa:

Visto l'art. 198 del regio decreto 16 marzo 1942, n. 267;

Viste, ai sensi dell'art. 9 della legge 17 luglio 1975, n. 400, le designazioni dell'associazione nazionale di rappresentanza alla quale il sodalizio risulta aderente;

Decreta:

Art. 1.

La società cooperativa «Dimensione Green Service Società cooperativa», con sede in Massa (codice 01155060112) è posta in liquidazione coatta amministrativa, ai sensi dell'art. 2545-terdecies del codice civile e la dott.ssa Serenella Di Donato, nata a Cagnano Amiterno (L'Aquila) il 31 ottobre 1960, domiciliata in Mariano Comense (Como), viale Lombardia, n. 58, ne è nominata commissario liquidatore.

Art. 2.

Al commissario nominato spetta il trattamento economico previsto dal decreto ministeriale 23 febbraio 2001, n. 64, pubblicato nella *Gazzetta Ufficiale* n. 72 del 27 marzo 2001.

Il presente decreto sarà pubblicato nella *Gazzetta Ufficiale* della Repubblica.

Tale provvedimento potrà essere impugnato dinanzi al competente tribunale amministrativo, ovvero in via straordinaria dinanzi al Presidente della Repubblica qualora sussistano i presupposti di legge.

Roma, 16 novembre 2009

Il Ministro: SCAIOLA

10A01317

