Gara a procedura ristretta per l'affidamento, mediante l'utilizzo dell'Accordo Quadro di cui all'art. 59 del D.Lgs. n. 163/2006, di Servizi di connettività per la Community Network RUPAR Puglia, nell'ambito del "Sistema Pubblico di Connettività - SPC" (CIG 53447009F5)

Allegato 1: Capitolato Tecnico

InnovaPuglia S.p.A.
St. prov. Casamassima Km 3
70010 Valenzano BARI
Italia
www.innova.puglia.it

Sommario

1 ACRONIMI

Si fornisce un elenco degli acronimi più frequentemente utilizzati nel presente documento con il relativo significato.

AAA	Autenticazione, Autorizzazione e Accounting
AgID	Agenzia per l'Italia Digitale
AS	Autonomous System
BGA	Banda Garantita in Accesso
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
CdS	Classe di Servizio
CN	Community Network
CTRP	Centro Tecnico RUPAR Puglia
DNS	Domain Name System
EPO	Exchange Point Operator
FSR	Fornitore Servizi RUPAR
NAP	Neutral Access Point
IDS/IPS	Intrusion Detection & Prevention System
NAT	Network Address Translation
NOC	Network Operation Centre
NTP	Network Time Protocol
OWD	One Way Delay
PA	Pubblica Amministrazione (centrale o locale)
PAC	Pubblica Amministrazione Centrale
PAL	Pubblica Amministrazione Locale
PAS	Punto di Accesso al Servizio
PBX	Private Branch eXchange
pps	Pacchetti per secondo
PSTN	Public Switched Telephone Network
QXN	Qualified eXchange Network
RTD	Round Trip Delay
RUPAR	Rete Unitaria della Pubblica Amministrazione Regionale
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOC	Security Operating Center
SPC	Sistema Pubblico di Connettività
TdR	Terminazione di Rete
TT	Trouble Ticket
VoIP	Voice Over IP
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

2 PREMESSA

La Community Network RUPAR-SPC Puglia (nel seguito CN RUPAR-SPC), come parte integrante del Sistema Pubblico di Connettività (SPC), ha per finalità l'interconnessione delle Pubbliche Amministrazioni Locali (PAL) pugliesi tra loro, con le Pubbliche Amministrazioni Centrali (PAC) e con le altre PAL interconnesse al SPC attraverso una infrastruttura di servizio che garantisca qualità e sicurezza delle connessioni, rispettando gli standard approvati a livello nazionale.

Il "Dominio di una PAL" potrà comprendere le seguenti reti:

- la rete interna (*Intranet*) che ospita le postazioni degli utenti che possono interconnettersi ad altre Amministrazioni e/o ad Internet;

- la DMZ (*DeMilitarized Zone*) destinata ad ospitare gli elaboratori (Service Hosts) preposti all'erogazione di servizi di applicativi offerti dall'Amministrazione agli utenti esterni (utenti Internet) ed ovviamente accessibili anche alle altre Amministrazioni;
- la RSR (*Rete dei Servizi RUPAR-SPC*) riservata ai servizi di interoperabilità e cooperazione applicativa tra Amministrazioni e quindi non accessibile da Internet ma solo dalle altre Amministrazioni connesse alla CN RUPAR-SPC o a SPC.

Il "Dominio di interconnessione della CN RUPAR-SPC" è rappresentato da un nodo detto EPO (Exchange Point Operator), ubicato presso il Parco Scientifico Tecnopolis, che consente di realizzare un peering locale tra i fornitori della CN RUPAR-SPC. L'EPO è completamente ridondato ed è esclusivamente riservato alla CN RUPAR-SPC e di conseguenza non gestito come punto di interconnessione riconosciuto dall'intero mondo Internet.

Il presente Capitolato descrive le specifiche tecniche di interconnessione ed operatività della CN RUPAR-SPC Puglia (nel seguito CN RUPAR-SPC) e definisce i requisiti tecnici minimi e le modalità di erogazione dei servizi oggetto della gara:

- **Servizi di Trasporto Dati**:
  - Servizi di Trasporto Dati Wired
  - Servizi di Trasporto Dati Wireless
- **Servizio di Posta Elettronica**
- **Servizi di Sicurezza**:
  - Servizi Di Sicurezza Perimetrale Unificata
  - Servizio Di Sicurezza Centralizzata
- **Servizi di Comunicazione Evoluta**
  - Servizi VOIP
  - Servizi di Telepresenza

Le caratteristiche tecniche e i requisiti di qualità (Service Level Agreement – SLA) dei servizi sopra indicati sono analoghi a quelli definiti da CONSIP nell'ambito della "Procedura ristretta per l'affidamento dei servizi di connettività nell'ambito del Sistema Pubblico di Connettività (SPC)" (di seguito indicata "Gara Multifornitore SPC"). Per questo i requisiti identici a quelli della "Gara Multifornitore SPC" mantengono la stessa codifica e numerazione di quella Gara (R.xx), quelli modificati mantengono la stessa posizione ma sono codificati come **RR.xx**., gli ulteriori requisiti (specifici della CN RUPAR-SPC) sono anch'essi codificati come **RR.xx**.

I Fornitori, una volta conseguita l'aggiudicazione definitiva parteciperanno al Accordo Quadro che fissa i termini e le condizioni di fornitura e, di conseguenza, si impegneranno a realizzare, in concorso tra loro, la CN RUPAR-SPC e saranno denominati Fornitori di Servizi della CN RUPAR-SPC Puglia (di seguito FSR). I FSR possono distinguersi in fornitori nazionali (di seguito FSR-n) o regionali (di seguito FSR-r): per fornitori nazionali si intendono i fornitori SPC aggiudicatari della "Gara Multifornitore SPC" oltre che dei servizi della presente gara, mentre per fornitori regionali si intendono gli altri fornitori aggiudicatari della presente gara.

3 PRESCRIZIONI GENERALI

[RR.1] I servizi devono essere aperti al cambiamento, cioè devono essere erogati in modo tale da consentire una facile introduzione di elementi innovativi risultanti dall'evoluzione della tecnologia o dalle mutazioni dei processi e delle esigenze delle Amministrazioni. Per questo i servizi oggetto del Contratto Quadro dovranno esser erogati utilizzando per quanto possibile soluzioni tecnologiche allo stato dell'arte in grado comunque di garantire la non obsolescenza nell'arco della durata del Contratto Quadro stesso.

[R.2] I servizi descritti si intendono comprensivi delle attività di fornitura, installazione, gestione, manutenzione, monitoraggio e implementazione delle politiche di sicurezza, inerenti tutte le componenti necessarie alla corretta erogazione dei servizi stessi come richiesto dal capitolato. Salvo quanto espressamente previsto nei listini, nessun onere derivante da queste attività e da quelle derivanti dalle misure tecnico-organizzative adottate per il monitoraggio e la rendicontazione dei livelli di servizio può essere richiesto dal Fornitore.

[R.3] I servizi sono caratterizzati da opportuni livelli di servizio (SLA) che ne prescrivono la qualità. I livelli di servizio richiesti sono descritti nell'Allegato 1.1 - Livelli di servizio e penali.

[R.4] Ai servizi oggetto del presente capitolato, salvo ove esplicitamente escluso, è associato un punto di accesso al servizio (PAS) che:

- individua il punto di consegna del servizio da parte del Fornitore
- delimita le frontiere di responsabilità del Fornitore e dell'Amministrazione
- è il punto di riferimento per la misura dei parametri di SLA.

Qualora il servizio non preveda PAS, la responsabilità del servizio è totalmente a carico del Fornitore e non esiste un punto di frontiera diretto tra infrastruttura per il servizio e quella dell'Amministrazione.

[R.5] Tutti i servizi nel presente capitolato includono attività di gestione e manutenzione (meglio descritte nel § 9) erogate all'interno della finestra temporale Lunedì-Venerdì, 08.00-20.00 e Sabato 08.00-14.00, festivi esclusi (finestra standard), salvo contrattualizzazione dell'opzione di "finestra di erogazione estesa" (cfr. [R.6]).

[R.6] Generalmente per ogni servizio è disponibile l'opzione finestra di erogazione estesa, che prevede l'adozione di una finestra di erogazione H24, in sostituzione della finestra di erogazione standard (lun. ven. 8:00 – 20:00, sab. 8:00 – 14:00) inclusa nel servizio base.

[RR.2] Il Fornitore deve acquisire il tempo ufficiale di rete attraverso il protocollo Network Time Protocol (NTP) versione 3 (o successive) tramite sincronizzazione con il servizio NTP propagato dal CTRP sulla CN RUPAR-SPC o tramite la sincronizzazione con il tempo di riferimento nazionale dell'Istituto Elettrotecnico Nazionale "Galileo Ferraris" come riferimento temporale assoluto ai fini della marcatura con "time stamp" dei log e dei trouble ticket, nonché per tutte le altre funzioni di gestione dei servizi che richiedono un riferimento temporale.

[R.8] L'installazione dei sistemi necessari per la fornitura dei servizi deve essere eseguita in conformità alle norme CEI attualmente in vigore, alle norme per la sicurezza degli impianti ed alle altre norme vigenti in materia.

[RR.3] Tutti i servizi nel presente capitolato devono essere forniti ad una Amministrazione in modo unitario dallo stesso FSR, con le uniche eccezioni dei servizi che sono esplicitamente indicati come servizi facoltativi e che possono essere richiesti dall'Amministrazione al Fornitore RUPAR-SPC, così come possono essere realizzati dall'Amministrazione in autonomia o mediante altro fornitore.

[RR.4] Il Fornitore, se richiesto dall'Amministrazione, deve distribuire senza alcun onere ai sistemi presenti nella RSR e nella DMZ il tempo ufficiale di rete acquisito secondo le modalità indicate al requisito [RR.2]. Il Fornitore deve altresì garantire la possibilità di sincronizzare un NTP Server interno all'Amministrazione per la sincronizzazione degli orologi di tutti i dispositivi della LAN interna dando origine ad una gerarchia di strati NTP.

4 SERVIZI DI TRASPORTO DATI

I servizi di trasporto dati sono dedicati alla trasmissione di qualunque tipo di dato (inclusi immagini e fonia) basati su protocollo IP.

I servizi di trasporto si articolano in:

- Servizi Wired:
  - Servizi di trasporto dati su portante elettrica (STDE);
  - Servizi di trasporto dati su portante ottica (STDO);
- Servizi Wireless:
  - Servizi di trasporto dati satellitari (STDS);
  - Servizi di trasporto dati Wimax (STDW);

- Servizi di trasporto dati Hiperlan (STDH).

[RR.5] I servizi di trasporto devono essere basati su Internet Protocol version IPv4 e IPv6. I servizi standard devono comprendere il trasporto e l'indirizzamento secondo la versione IPv4. L'Amministrazione cliente può richiedere, senza differenze di prezzo, che il servizio venga fornito secondo gli standard IPv6 o con sistemi configurati con dual stack IPv4/IPv6.

[R.10] Il Fornitore deve garantire soluzioni conformi alle normative e agli standard vigenti, aggiornate allo stato dell'arte della tecnologia disponibile ed in linea con l'evoluzione degli standard di riferimento ove applicabili (es. IETF, IEEE, ecc.).

[R.11] Le interfacce per la fruizione dei servizi devono essere conformi ai relativi standard de jure e de facto, come richiesto all'interno delle specifiche relative ad ogni servizio oggetto di fornitura.

[RR.6] Relativamente al trasporto del traffico IP sono definiti nella CN RUPAR-SPC i seguenti ambiti:

- Intranet: un ambito costituito dal dominio interno alla singola Amministrazione che connette tutte le sedi (o un sottoinsieme delle stesse) della stessa;
- Infranet: un ambito di interconnessione che connette tra loro le PAL della CN RUPAR-SPC e le altre Amministrazioni SPC non appartenenti alla CN RUPAR-SPC sia assegnate allo stesso fornitore che, tramite la QXN e l'infrastruttura della CN RUPAR-SPC, a fornitori diversi secondo le modalità definite nel § 10.2;
- RUPAR: un ambito di interconnessione che connette tra loro le PAL pugliesi sia assegnate allo stesso FSR che, tramite l'infrastruttura della CN RUPAR, a FSR diversi secondo le modalità definite nel § 10.1; si tratta di una specializzazione dell'ambito Infranet che si avvale di specifiche infrastrutture realizzate sul territorio regionale;
- Internet: un ambito di interazione tra le singole Amministrazioni e soggetti non afferenti al SPC, attraverso la rete Internet.

[R.13] Il Fornitore deve garantire, su accessi configurati per gestire più ambiti, la segregazione del traffico appartenente a ciascun ambito.

[R.14] Tutti i servizi di trasporto dati definiti nel presente capitolato includono nel servizio base l'ambito Intranet.

[RR.7] I servizi di trasporto dati in ambito Intranet sono facoltativi.

[R.15] Ogni Amministrazione dovrà dotarsi di almeno un collegamento in ambito Infranet.

[RR.8] Ogni Amministrazione dovrà dotarsi di almeno un collegamento in ambito RUPAR.

[RR.9] La connettività verso tutti gli ambiti deve essere fornita senza limitazioni temporali e di accesso ai contenuti (network neutrality), anche da parte dei subfornitori e fino ai backbone internazionali; il Fornitore non può autonomamente limitare il trasporto di alcun protocollo dell'intera suite di protocolli Internet. Il fornitore in accordo con l'Amministrazione, deve comunque tenere conto delle eventuali indicazioni di AgID, del CTRP e del Cert della P.A. in merito a comportamenti da assumere in relazione a traffico anomalo ed a minacce.

[R.17] Gli apparati di accesso forniti con i servizi di trasporto, ove previsti, devono essere gestiti e configurati dal Fornitore come componenti integranti del servizio, devono pertanto:

- essere ricompresi nel prezzo offerto;
- essere allo stato dell'arte della tecnologia e del mercato;
- implementare protocolli allo stato dell'arte;
- essere dimensionati in modo da garantire il rispetto dei livelli di servizio previsti.

[R.18] Non devono essere adottate politiche di traffic shaping sugli apparati di accesso, che impediscano, in assenza di congestione, di utilizzare la larghezza di banda massima del circuito di accesso.

[RR.10] I parametri che caratterizzano i servizi di trasporto dati sono:

- **BNA (Banda Nominale in Accesso)**: definita come la banda fisica configurata sull'interfaccia geografica del servizio in oggetto. Relativamente ai soli servizi STDE, STDS e STDW, la BNA prevede una differenziazione in termini di banda nominale in uplink (BNAU) e di banda nominale in downlink (BNAD).
- **BGA (Banda Garantita in Accesso)**: definita come la larghezza di banda IP (comprensiva dell'overhead di protocollo) simmetrica in uplink e downlink garantita dal Fornitore. La BGA costituisce quindi il massimo valore di throughput per il quale il Fornitore è obbligato alla garanzia dei parametri di performance indicati per ciascuna tipologia di servizio (cfr. Allegato 1.1 - Livelli di servizio e penali).

[R.20] I servizi di trasporto dati di base, privi quindi della sottoscrizione di opzioni aggiuntive, devono comprendere:

- l'apparato di accesso al servizio;
- il circuito che permette all'Amministrazione il collegamento alla rete del Fornitore;
- l'abilitazione all'ambito Intranet (disattivabile su richiesta);
- la garanzia del trasporto di flussi di traffico fino al raggiungimento della BGA (se prevista dallo specifico servizio);
- il trasporto in modalità best effort, fino al raggiungimento della BNA;
- il rispetto dei livelli di assurance nella "finestra di erogazione standard".

[R.21] Il Punto di accesso al servizio (PAS) per i servizi di trasporto dati è definito come l'insieme delle interfacce lato utente messe a disposizione dal Fornitore sugli apparati di terminazione del servizio in sede della Amministrazione.

[RR.11] I servizi di trasporto comprendono anche l'erogazione di un servizio Domain Name System (DNS) che consenta sia la pubblicazione dei nomi a dominio delle Pubbliche Amministrazioni che la risoluzione dei nomi a dominio, relativi ai soli ambiti RUPAR/Infranet e Internet. Il servizio deve essere disponibile sia in caso di IPv4 che di IPv6.

[RR.12] Il servizio DNS ha sempre una finestra di erogazione estesa, indipendentemente dai servizi di trasporto dati contrattualizzati.

[RR.13] L'organizzazione del servizio di gestione DNS nella CN RUPAR Puglia prevede:

- che ogni FSR recepisca le eventuali modificazioni alle regole tecniche di gestione del naming nella CN RUPAR Puglia, se queste fossero finalizzate a migliorare il servizio complessivo;
- che ogni FSR garantisca la fruizione del servizio di risoluzione a tutte le postazioni del Dominio Amministrativo fornendo modalità tecniche di utilizzo all'utenza;
- che ogni FSR coordini la gestione del naming per tutte le reti (DMZ, Intranet, RSR); in particolare, per un host raggiungibile da più reti (ad es. dalla rete Intranet della generica PAL e dalla rete Internet) deve essere utilizzato sempre lo stesso nome simbolico;
- che ogni FSR, se richiesto dall'Amministrazione o dal CTRP, al fine di garantire la continuità dei servizi in caso di disastro, deve riservare indirizzi IP alternativi e deve mantenere (e in caso di necessità applicare) file di configurazione DNS alternativi;
- che ogni FSR predisponga sulla Intranet, soltanto se richiesto dalla PAL, il DNS server primario e secondario per il nome del dominio individuato dalla PAL, predisponendo meccanismi di *forward* e/o *chaching* per risolvere nomi esterni.

[RR.14] Per l'erogazione del servizio DNS nella CN RUPAR-SPC è prevista l'allocazione di due DNS Server esclusivamente dedicati presso il Centro Servizi del FSR o presso l'EPO.

[RR.15] Il sistema DNS del Fornitore deve essere configurato in modo tale da essere suddiviso in due componenti Internet e RUPAR/Infranet per la gestione differenziata di ciascun ambito.

[RR.16] La componente DNS Internet deve risolvere i nomi per le zone di propria competenza sulla sola rete Internet; nessun nome di host presente sulla Intranet e/o sulla rete RSR deve essere risolto attraverso l'ambito internet.

[RR.17] Per quanto riguarda la componente DNS RUPAR/Infranet:

- il CTRP gestisce il dominio **rsr.rupar.puglia.it**, dominio riservato al censimento dei **Domini di Cooperazione Applicativa**;
- per ogni Amministrazione, il Fornitore deve chiedere al CTRP la delega per l'attivazione del dominio RUPAR "***nome_ente*.rsr.rupar.puglia.it**";
- per ciascun dominio "***nome_ente*.rsr.rupar.puglia.it**" i Fornitori sono obbligati ad attivare tre *Name Server* (uno primario/master e due secondari/slave);
- il Fornitore deve gestire sia il *Primary Name Server* del dominio "***nome_ente*.rsr.rupar.puglia.it**" che uno dei due *Name Server* secondari;
- il Fornitore deve definire come altro *Name Server* secondario il *Primary Name Server* del CTRP, gestore del dominio di livello più alto "**rsr.rupar.puglia.it**";
- nella zona "***nome_ente*.rsr.rupar.puglia.it**" vengono censiti gli host per la cooperazione applicativa e tutti gli IP# riservati, assegnati a componenti della Porta di Rete (PdR) dell'Amministrazione.
- i Fornitori registreranno e gestiranno i domini *"**<nomeFSR>**.rsr.rupar.puglia.it*" per censire i nomi simbolici assegnati ai propri apparati di rete.

[RR.18] La componente DNS RUPAR/Infranet deve essere configurata in modo tale da annunciare automaticamente verso il *Primary Name Server* del CTRP il cambiamento di una zona di propria competenza, attraverso l'utilizzo del meccanismo DNS Notify (RFC1996). Inoltre il sistema DNS del Fornitore deve essere configurato in modo tale da accettare le richieste di AXFR (Full Zone Transfer) e IXFR (Incremental Zone Transfer RFC1995), provenienti dal *Primary Name Server* del CTRP.

[R.27] Il sistema DNS deve essere configurato in modo da accettare lo Zone Transfer da parte dei sistemi DNS delle Amministrazioni, in modo da garantire la pubblicazione automatica dei nomi a dominio di loro competenza, tramite i meccanismi di DNS Notify (RFC1996).

[R.28] Il Fornitore deve garantire altresì la gestione dei change dei nomi a dominio su richiesta dell'Amministrazione.

[R.30] Il sistema DNS deve implementare meccanismi di cache per la risoluzione dei nomi, e meccanismi di forwarding selettivo su base dominio.

[RR.19] Il Fornitore dovrà garantire la memorizzazione in "cache" (durata infinita) nei propri DNS dei DNS del CTRP autoritativi per il dominio "rsr.rupar.puglia.it".

[RR.20] Il piano di indirizzamento adottato nell'ambito della CN RUPAR-SPC deve garantire l'univocità degli indirizzi IPv4 e/o IPv6 attribuiti ai singoli sistemi.

[RR.21] Ciascun Fornitore deve definire un blocco di indirizzi IP pubblici da riservare alle RSR delle Amministrazioni clienti ed un blocco distinto, sempre con indirizzi IP pubblici, da riservare per le DMZ.

[RR.22] Oltre a quelli eventualmente necessari per la gestione delle proprie Terminazioni di Rete (TdR), il FSR deve rendere disponibili, a richiesta dall'Amministrazione, al fine di realizzare servizi esposti su RUPAR/Infranet o Internet, almeno il numero di indirizzi IPv4 pubblici correlato al numero complessivo di accessi wired e wireless contrattualizzati secondo quanto indicato nella tabella successiva.

Numero di accessi contrattualizzati	Numero di indirizzi disponibili
Fino a 2	8
Da 3 a 10	16
Da 11 a 25	32
Da 26 a 50	64
Da 51 a 100	128
Da 101 a 200	256
Oltre 200	512

Non vi sono invece limiti specifici sul numero di indirizzi IPv6 pubblici che il Fornitore deve rendere disponibili all'Amministrazione.

[RR.23] Le postazioni dell'Intranet di un'Amministrazione hanno indirizzi IP privati e l'accesso alla CN RUPAR-SPC o ad Internet dovrà essere garantito da un Proxy, responsabile anche di "nascondere" gli indirizzi degli elaboratori interni, rendendo noto all'esterno esclusivamente il proprio indirizzo.

[RR.24] Il Proxy, per consentire alle stazioni dell'Intranet di una Amministrazione l'accesso ai servizi della CN RUPAR-SPC, deve assumere all'esterno un indirizzo IP pubblico della rete RSR.

[RR.25] Sui servizi di trasporto dati, oltre l'ambito Intranet, incluso di default e disattivabile su richiesta, può essere prevista un'opzione **Multiambito** che permette l'abilitazione del traffico dati sugli ambiti RUPAR, Infranet ed Internet. Ognuno degli ambiti, su richiesta dell'Amministrazione, deve poter essere disabilitato separatamente, tenuto conto dei requisiti [R.15] e [RR.8].

4.1 Precondizioni e vincoli per la sottoscrizione dei servizi STD

[RR.26] L'opzione Multiambito richiede obbligatoriamente garanzie di sicurezza, pertanto per l'attivazione di tale opzione deve essere assicurata, sull'accesso per il quale viene richiesta, almeno una delle seguenti condizioni:

- sottoscrizione di un Servizio di Sicurezza Centralizzata (SCEN) (di cui al § 6.1.2), se compatibile col profilo del servizio di trasporto richiesto;
- sottoscrizione di almeno un Servizio di Sicurezza Perimetrale Unificata (SPUN) (di cui al § 6.1.1);
- implementazione di sistemi di sicurezza propri in grado di garantire almeno le seguenti funzionalità di sicurezza:
  - firewalling;
  - intrusion detection;
  - monitoraggio e registrazione degli eventi di sicurezza.

[RR.27] In quest'ultimo caso il Fornitore contestualmente alla richiesta dell'Amministrazione deve far compilare alla medesima un documento di dichiarazione che attesti detta implementazione da parte dell'Amministrazione.

4.2 Servizi di trasporto wired

[R.34] I servizi di trasporto di tipo wired sono caratterizzati da collegamenti fisici permanenti tra le sedi delle Amministrazioni e la rete del Fornitore.

[R.35] I servizi di traporto di tipo wired richiesti al Fornitore sono di due tipi:

- **Servizi di Trasporto Dati su portante Elettrica (STDE)**: di tipo always-on, in cui il rilegamento fisico utilizzato per il circuito di accesso è costituito da uno o più doppini in rame. E' ammessa la realizzazione dei medesimi servizi anche tramite collegamenti in fibra ottica.
- **Servizi di Trasporto Dati su portante Ottica (STDO)**: di tipo always-on, in cui il rilegamento fisico utilizzato per il circuito di accesso è realizzato in fibra ottica.

[R.36] Per ciascun servizio, il Fornitore deve mettere a disposizione dell'Amministrazione uno o più apparati di accesso, con una o più interfacce fisiche lato utente compatibili con l'infrastruttura di rete dell'Amministrazione (ognuna di tali interfacce deve essere conforme ad uno dei seguenti standard: Fast Ethernet 10/100 Autosensing, Gigabit Ethernet o 10Gigabit Ethernet).

[R.37] La capacità totale delle interfacce lato utente non può essere inferiore alla BNA contrattualizzata sull'accesso (in caso di accesso asimmetrico della maggiore tra BNAU e BNAD).

[R.38] Gli apparati di accesso forniti con i servizi devono garantire una capacità di commutazione in termini di pacchetti al secondo (CCP) pari a quella indicata per ciascun profilo di servizio secondo quanto riportato in [R.41] per STDE e in [R.49] per STDO.

[R.39] Sul medesimo apparato di accesso fornito con i servizi di trasporto dati wired, su richiesta dell'Amministrazione, possono essere configurati uno o più ambiti.

4.2.1 Servizi di Trasporto Dati su Portante Elettrica (STDE)

[R.41] I servizi STDE prevedono la fornitura di servizi di trasporto dati su protocollo IP (IPv4 e/o IPv6) con le caratteristiche indicate nella seguente tabella:

Profilo	BNA Down/Uplink		BGA		CCP (Kpps)
STDE-A1	640/128	Kbps	64	Kbps	-
STDE-A2	1024/128	Kbps	64	Kbps	-
STDE-A3	1024/256	Kbps	128	Kbps	-
STDE-A4	2048/256	Kbps	128	Kbps	-
STDE-A5	2048/512	Kbps	256	Kbps	-
STDE-A6	4096/512	Kbps	256	Kbps	-
STDE-A7	10240/1024	Kbps	512	Kbps	1
STDE-A8	20480/1024	Kbps	512	Kbps	1
STDE-A9	30/3	Mbps	512	Kbps	1
STDE-A10	30/3	Mbps	1.024	Kbps	8
STDE-S1	2048/2048	Kbps	256	Kbps	0,5
STDE-S2	2048/2048	Kbps	384	Kbps	0,75
STDE-S3	2048/2048	Kbps	512	Kbps	1
STDE-S4	2048/2048	Kbps	1024	Kbps	2
STDE-S5	4096/4096	Kbps	2048	Kbps	4

STDE-S6	8192/8192	Kbps	4096	Kbps	8

[R.42] I servizio STDE prevede accessi:

- asimmetrici (profili da STDE-A1 a STDE-A10), caratterizzati cioè da BNAU<BNAD;
- simmetrici (profili da STDE-S1 a STDE-S6), caratterizzati cioè da BNA=BNAU=BNAD.

[R.43] I servizi di trasporto di tipo STDE

- asimmetrici a bassa velocità (profili da STDE-A1 a STDE-A8), devono essere erogati con copertura geografica almeno coincidente con quella del servizio Wholesale Bitstream ADSL dell'operatore notificato per servizi con identica BNA, aggiornando la disponibilità dei servizi nel caso in cui l'offerta Wholesale Bitstream venga estesa durante la durata del contratto. Nel caso in cui, durante la durata del contratto AGCOM non ritenesse giustificata un'offerta Wholesale Bitstream in aree servite attraverso l'offerta di accesso disaggregato alla rete in rame (ULL), l'obbligo di fornitura includerà anche le aree coperte solo dalla succitata offerta di accesso disaggregato;
- asimmetrici ad alta velocità (profili da STDE-A9 a STDE-A10), devono essere erogati con copertura geografica almeno coincidente con quella del servizio Wholesale Bitstream NGA in modalità FTTCab dell'operatore notificato;
- simmetrici (profili da STDE-S1 a STDE-S6), devono essere erogati con copertura geografica almeno coincidente con quella del servizio Wholesale Bitstream SHDSL dell'operatore notificato per servizi con identica BNA, aggiornando la disponibilità dei servizi nel caso in cui l'offerta Wholesale Bitstream venga estesa durante la durata del contratto. Nel caso in cui, durante la durata del contratto AGCOM non ritenesse giustificata un'offerta Wholesale Bitstream in aree servite attraverso l'offerta di accesso disaggregato alla rete in rame (ULL), l'obbligo di fornitura includerà anche le aree coperte solo dalla succitata offerta di accesso disaggregato.

4.2.1.1 Opzioni dei servizi STDE

[RR.28] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di trasporto dati STDE:

- **Affidabilità elevata** (cfr. [R.45]);
- **Multiambito** (cfr. [RR.25]);
- **Estensione apparato Wi-Fi** (cfr. 4.5);
- **Backup** (cfr. § 4.6);
- **Finestra di erogazione estesa** (cfr. [R.6]);
- **Servizi di Banda Riservata (SBRI)** (cfr. § 4.4).

[R.45] L'opzione Affidabilità elevata prevede che il servizio sia realizzato ridondando completamente la soluzione tecnologica caratterizzante il servizio base in modo da garantire, in caso di guasto singolo, funzionalità e prestazioni equivalenti. La soluzione consiste in un accesso secondario equivalente all'accesso primario (quello incluso con il servizio base di cui al [R.20] con i profili di cui al [R.41]) con realizzazione del collegamento tale da minimizzare i singoli punti di guasto. Sugli apparati di accesso, devono essere implementati meccanismi di tipo active-standby, pertanto solo in caso di indisponibilità dell'accesso primario, il traffico è instradato sull'accesso secondario. L'opzione deve garantire, nella centrale del Fornitore, l'attestazione dei circuiti di accesso su apparati differenti. Entrambe le componenti del servizio devono essere monitorate e gestite. Gli SLA del servizio per quanto riguarda i parametri di assurance sono differenziati rispetto al servizio base (cfr. Allegato 1.1 - Livelli di servizio e penali).

4.2.2 Servizi di Trasporto Dati su Portante Ottica (STDO)

[R.49] Il servizio di trasporto di tipo STDO prevede la fornitura di servizi di trasporto dati su protocollo IP (IPv4 e/o IPv6) con le caratteristiche indicate nella seguente tabella:

Profilo	BNA		BGA		CCP (Kpps)
STDO-1	10	Mbps	10	Mbps	15
STDO-2	20	Mbps	20	Mbps	30
STDO-3	40	Mbps	40	Mbps	60
STDO-4	100	Mbps	100	Mbps	150
STDO-5	200	Mbps	200	Mbps	300
STDO-6	300	Mbps	300	Mbps	450
STDO-7	600	Mbps	600	Mbps	900
STDO-8	1	Gbps	1	Gbps	1.500
STDO-9	2,5	Gbps	2,5	Gbps	3.000
STDO-10	5	Gbps	5	Gbps	5.000
STDO-11	10	Gbps	10	Gbps	6.000

[R.50] Il servizio di trasporto di tipo STDO prevede accessi simmetrici, caratterizzati cioè da BGA=BGAU=BGAD.

[RR.29] I servizi di trasporto di tipo STDO devono essere erogati in tutti i punti del territorio in cui è disponibile l'offerta Wholesale Bitstream NGA in modalità FTTH dell'operatore notificato.

4.2.2.1 Opzioni dei servizi STDO

[RR.30] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di trasporto dati STDO:

- **Affidabilità eleva**ta (cfr. [RR.31]);
- **Multiambito** (cfr. [RR.25]);
- **Estensione apparato Wi-Fi** (cfr. 4.5);
- **Backup** (cfr. § 4.6);
- **Finestra di erogazione estesa** (cfr. [R.6]).
- **Servizi di Banda Riservata** (SBRI) (cfr. § 4.4).

[RR.31] L'opzione Affidabilità elevata prevede che il servizio sia realizzato ridondando completamente la soluzione tecnologica caratterizzante il servizio base in modo da garantire, in caso di guasto singolo, funzionalità e prestazioni equivalenti. La soluzione consiste in un accesso secondario equivalente all'accesso primario (quello incluso con il servizio base di cui al [R.20] e i profili di cui al [R.49]), ma con instradamento fisico differente, in modo da minimizzare i singoli punti di guasto. L'opzione affidabilità elevata per i servizi STDO prevede il *load balancing*, consistente nell'implementazione di politiche di bilanciamento di carico fra i due distinti apparati di accesso contrattualizzati con l'adesione all'opzione. La soluzione deve essere comprensiva degli ulteriori apparati necessari all'implementazione delle politiche di *load balancing,* non già previsti dalla soluzione base; le funzionalità di *load balancing* possono essere anche implementate attraverso opportuna configurazione delle terminazioni di rete. In caso di utilizzo di architetture basate su bilanciatori esterni, tali bilanciatori su richiesta dell'Amministrazione, possono anch'essi essere ridondati. L'opzione deve garantire nella centrale del Fornitore l'attestazione dei circuiti di accesso su apparati differenti o laddove disponibile, per accessi con BNA ≥ 100 Mbps, il *dual-homing* (attestazione dei circuiti di accesso su PoP distinti del Fornitore). Entrambe le

componenti del servizio devono essere monitorate e gestite. Gli SLA del servizio per quanto riguarda i parametri di assurance sono differenziati rispetto al servizio base (cfr. Allegato 1.1 - Livelli di servizio e penali).

4.3 Servizi di trasporto dati wireless

[R.72] I servizi di trasporto di tipo wireless sono caratterizzati da collegamenti radio tra sedi delle Amministrazioni e la rete del Fornitore.

[RR.32] I servizi di trasporto di tipo wireless che devono essere erogati dal Fornitore sono:

- **Servizi di Trasporto Dati Satellitari (STDS)**: di tipo always-on, consentono il collegamento di una sede dell'Amministrazione attraverso un canale satellitare.
- **Servizi di Trasporto Dati Wimax (STDW)**: di tipo always-on, consentono il collegamento di una sede dell'Amministrazione attraverso un accesso di tipo wireless su banda licenziata secondo lo standard IEEE 802.16.
- **Servizi di Trasporto Dati Hiperlan (STDH)**: di tipo always-on, consentono il collegamento di una sede dell'Amministrazione attraverso un accesso di tipo wireless su banda non licenziata secondo lo standard ETSI Hiperlan.

4.3.1 Servizi di Trasporto Dati Satellitare (STDS)

[RR.33] I servizi STDS prevedono la fornitura di servizi di trasporto dati su protocollo IP attraverso collegamenti satellitari bidirezionali costituiti da profili asimmetrici, con le caratteristiche BNA 20 / 6 Mbpsec, rispettivamente in Downlink e in Uplink.

[RR.34] I servizi di trasporto di tipo STDS erogati in tecnologia satellitare sono comprensivi:

- del collegamento fra il satellite e l'Amministrazione;
- del collegamento fra il satellite e la rete del Fornitore;
- delle parabole e dei cablaggi necessari per la fruizione del servizio fino ad un massimo di 50 metri (l'Amministrazione richiedente deve rendere disponibile, per ciascuna sede su cui è richiesto il servizio, appositi spazi per l'installazione delle parabole che assicurino la visibilità del satellite ed eventuali autorizzazioni necessarie per i cablaggi);
- dell'apparato di attestazione in sede dell'Amministrazione;
- della componente di traffico caratterizzata da velocità di picco con throughput fino all'intero valore di BNA definito per il singolo accesso, banda minima garantita down/up con e per un volume di traffico incluso nel canone mensile pari a quanto indicato in [RR.36] in termini di GByte/mese(download + upload).

[R.76] L'apparato di attestazione deve essere in grado di interfacciarsi con la LAN o singoli PC almeno attraverso interfacce Fast Ethernet (10/100 Autosensing).

[R.77] I servizi STDS non sono caratterizzati da alcuna limitazione in termini di copertura geografica sul territorio nazionale.

[R.78] Per i servizi STDS non è previsto il Servizio di Banda Riservata (SBRI) e l'intera banda viene pertanto trattata esclusivamente in modalità Best Effort. Pacchetti appartenenti a diverse CdS devono comunque essere trasportati ma a questi non sono applicati degli SLA prestazionali differenziati.

[R.80] Il Fornitore deve installare nella singola sede dell'Amministrazione sistemi trasmissivi che garantiscano una velocità almeno pari alla BNA definita per ciascun profilo in Upload (trasmissione) e in Download (ricezione).

[R.81] Il Fornitore deve garantire che, almeno in alcuni momenti, sia possibile l'utilizzo dell'intera BNA.

[RR.35] Al fine di considerare il servizio disponibile, la banda messa a disposizione per ogni singolo accesso non deve essere mai inferiore al valore di Banda minima garantita all'interno della soglia di volume di traffico in Giga Byte mensile. Al superamento di una soglia di traffico (somma di trasmissione e ricezione) su base mensile la banda disponibile in modalità Best Effort può essere ridotta al valore BBE (Banda Best Effort) riportata nella tabella del [RR.36]. L'intera disponibilità della BNA deve essere ripristinata al termine del periodo mensile di riferimento.

[RR.36] Per ciascuna tipologia di profilo i valori di riferimento per le soglie e le BBE sono indicate in tabella:

Profilo	BNA		BGA		Volume di traffico mensile GB		BBE	
	(Down/ Uplink in Mbps)		(Down/Uplink in Kbps)		07:00 – 23:00	23:00 – 07:00	(Down/ Uplink in Kbps)	
STDS-1	20	6	32	32	15	flat	256	128
STDS-2	20	6	64	32	25	flat	256	128
STDS-3	20	6	128	64	50	flat	512	128

[R.84] Il Fornitore ha la possibilità, previa autorizzazione dell'Amministrazione, di limitare o bloccare alcune tipologie di traffico anomalo non collegate ad applicazioni di interesse dell'Amministrazione stessa.

4.3.1.1 Opzioni dei servizi STDS

[RR.37] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di trasporto dati STDS:

- **Multiambito** (cfr. [RR.25]);
- **Estensione apparato Wi-Fi** (cfr. 4.5);
- **Finestra di erogazione estesa** (cfr. [R.6]).

4.3.2 Servizi di Trasporto Dati Wimax (STDW)

[RR.38] I servizi STDW prevedono la fornitura di servizi di trasporto dati su protocollo IP attraverso collegamenti Wimax bidirezionali costituiti da un profilo asimmetrico, con le caratteristiche indicate nella seguente tabella:

Profilo	BNA Down/Uplink		BGA	
STDW	7/1	Mbps	512	Kbps

[RR.39] I servizi di trasporto di tipo STDW erogati sono comprensivi:

- di uno o più apparati di accesso (con funzionalità anche di *Subscriber Station* – SS), con una o più interfacce fisiche lato utente compatibili con l'infrastruttura di rete dell'Amministrazione; ognuna di tali interfacce deve essere conforme allo standard Fast Ethernet 10/100 Autosensing;

- dei cablaggi necessari per la fruizione del servizio fino ad un massimo di 50 metri.

[RR.40] Sul medesimo apparato di accesso fornito con il servizio STDW, su richiesta dell'Amministrazione, possono essere configurati uno o più ambiti.

4.3.2.1 Opzioni dei servizi STDW

[RR.41] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di trasporto dati STDS:

- **Multiambito** (cfr. [RR.25]);
- **Estensione apparato Wi-Fi** (cfr. 4.5);
- **Finestra di erogazione estesa** (cfr. [R.6]).

4.3.3 Servizi di Trasporto Dati Hiperlan (STDH)

[RR.42] I servizi STDH prevedono la fornitura di servizi di trasporto dati su protocollo IP attraverso collegamenti Hiperlan bidirezionali costituiti da profili simmetrici, con le caratteristiche indicate nella seguente tabella:

Profilo	BNA		BGA	
STDH-1	2	Mbps	1	Mbps
STDH-2	4	Mbps	2	Mbps
STDH-3	8	Mbps	4	Mbps
STDH-4	10	Mbps	5	Mbps
STDH-5	20	Mbps	10	Mbps
STDH-6	40	Mbps	20	Mbps
STDH-7	100	Mbps	50	Mbps

[RR.43] I servizi di trasporto di tipo STDH erogati sono comprensivi:

- di uno o più apparati di accesso, con una o più interfacce fisiche lato utente compatibili con l'infrastruttura di rete dell'Amministrazione; ognuna di tali interfacce deve essere conforme allo standard Fast Ethernet 10/100 Autosensing;
- dei cablaggi necessari per la fruizione del servizio fino ad un massimo di 50 metri.

[RR.44] Essendo previste per i servizi STDH comunicazioni in porzioni di spettro libere da licenza, il Fornitore deve eseguire per ogni Amministrazione un'attività di pianificazione radio attraverso:

- l'analisi delle bande effettivamente disponibili;
- sopralluoghi dedicati alla misura dei livelli di interferenza nelle bande di operazione e nelle bande ad essa adiacenti, dovuta sia agli utenti presenti nell'area sia ad interferenti accidentali, nonché alla determinazione delle caratteristiche del collegamento (individuazione degli ostacoli) tra trasmettitore e ricevitore;
- una volta completata l'analisi a radiofrequenza e installati i terminali radio agli estremi del collegamento, una fase di valutazione delle prestazioni del collegamento effettuata in termini di:

- throughput,
- latenza,
- tasso di perdita di pacchetto,
- numero di ritrasmissioni.

[RR.45] Per garantire qualità ed efficienza dei collegamenti realizzati per le Amministrazioni, il Fornitore deve monitorare puntualmente le installazioni radio in modo da poter procedere proattivamente all'esecuzione di eventuali azioni correttive in caso di decremento dell'efficienza operativa o delle performance del collegamento. Rientrano tra queste azioni la modifica dei parametri operativi dei collegamenti e l'eventuale cambio di topologia o di tecnologia.

4.3.3.1 Opzioni dei servizi STDH

[RR.46] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di trasporto dati STDS:

- **Multiambito** (cfr. [RR.25]);
- **Estensione apparato Wi-Fi** (cfr. 4.5);
- **Finestra di erogazione estesa** (cfr. [R.6]).

4.4 Opzione dei servizi di trasporto dati: Servizio di Banda Riservata (SBRI)

[RR.47] La componente opzionale Servizio di Banda Riservata (SBRI), garantisce parametri qualitativi differenziati a seconda della tipologia di traffico in transito su un servizio di trasporto dati wired. I parametri qualitativi di cui è garantito il rispetto sono i seguenti:

- ***Round Trip Delay (RTD)***: tempo di percorrenza necessario ad un pacchetto per percorrere la tratta origine-destinazione-origine;
- ***Packet Loss (PL)***: tasso di perdita dei pacchetti, rapporto espresso in percentuale tra il numero di pacchetti non consegnati e numero di pacchetti trasmessi in una tratta origine-destinazione;
- ***Packet Delay Variation (PDV)***: variazione in valore assoluto del ritardo tra due pacchetti consecutivi.
- La componente opzionale SBRI prevede 5 profili definiti nella seguente tabella. I profili SBRI-1, SBRI-2, SBRI-3 e SBRI-4, fanno riferimento a modalità di trasmissione di tipo Unicast, mentre il profilo SBRI-5 fa riferimento a modalità di trasmissione di tipo Multicast:

Profilo	Classe di servizio
SBRI-1	Real Time
SBRI-2	Mission Critical
SBRI-3	Streaming
SBRI-4	Multimedia
SBRI-5	Multicast

Nel caso di comunicazioni tra sedi di Amministrazioni servite da Fornitori diversi per tratta origine-destinazione si intende la tratta che va dalla Terminazione di Rete (TDR) che realizza il Punto di Accesso al Servizio (PAS) al Border Router interconnesso all'EPO per l'ambito RUPAR, al Border Router Internet per l'ambito Internet e, per l'ambito Infranet, al Border Router interconnesso alla QXN o al nodo di peering verso la QXN della CN RUPAR-SPC rispettivamente per i fornitori nazionali o regionali.

[R.56] La componente opzionale SBRI è sottoscrivibile unicamente per i servizi STDE e STDO.

[RR.48] In funzione delle applicazioni trasportate, sono definite le seguenti Classi di Servizio (CdS) con i corrispondenti valori minimi accettabili per ciascuna caratteristica di qualità:

CdS	RTD	PL	PDV
Real Time (RT)	< 65 ms	< 0,1%	<10 ms
Mission Critical (MC)	< 100 ms	< 0,1%	-
Streaming (ST)	< 400 ms	< 0,5%	<250 ms
Multimedia (MM)	< 500 ms	< 5%	-
Multicast	-	< 0,5%	-

[RR.49] La componente opzionale SBRI, deve essere in grado di assegnare una delle cinque possibili classi di servizio a ciascun pacchetto in transito (esclusi i pacchetti relativi all'ambito Internet e quelli di tipo best effort), secondo politiche basate su:

- indirizzo IP di origine;
- indirizzo IP di destinazione;
- protocollo applicativo utilizzato;
- interfaccia LAN dell'apparato d'accesso (su richiesta dell'Amministrazione è possibile erogare il servizio SBRI su interfacce LAN separate dell'apparato d'accesso);
- una combinazione delle precedenti.

[R.59] La somma delle componenti SBRI associate ad un servizio non può eccedere la BGA propria dello specifico servizio, cioè:

$$\sum_{i=1}^{5} SBRI_i \leq BGA$$

[RR.50] La componente SBRI di tipo Real Time contrattualizzabile non può essere superiore al 35% della BGA (in blocchi di 64 Kbps). Pertanto, per quanto riguarda il trasporto del traffico Real Time di cui alla componente SBRI:

- per profili asimmetrici STDE da A1 a A4 non è possibile contrattualizzare la componente SBRI di banda riservata Real Time;
- per i profili STDE A5, A6 e S1 è possibile contrattualizzare una sola componente SBRI di banda riservata Real Time composta da un unico blocco da 64 Kbps;
- per gli altri servizi STDE e per tutti servizi STDO è possibile contrattualizzare più di una componente SBRI e più blocchi di banda riservata Real Time fino al 35% della BGA.

[R.61] L'apparato d'accesso fornito con i servizi di trasporto dati per i quali è stata sottoscritta la componente opzionale SBRI1, deve essere in grado di gestire il traffico attraverso un meccanismo di accodamento prioritario che, in caso di saturazione della banda associata alla suddetta componente, deve prevedere lo scarto dei pacchetti in eccesso; il traffico delle componenti SBRI-2, SBRI-3 e SBRI-4, deve essere gestito equamente, e in caso di saturazione delle bande associate alle suddette componenti, essere declassato a traffico Best Effort.

[R.62] Le componenti SBRI che prevedono una modalità di trasmissione di tipo Multicast possono essere utilizzate dalle Amministrazioni che hanno necessità di inviare flussi di informazione da una o più sorgenti verso un gruppo di più riceventi, per il solo ambito Intranet.

[R.63] L'architettura del servizio utilizzata dal fornitore dovrà essere in grado di supportare il multicast secondo gli standard Protocol Indipendent Multicast – Sparse Mode (PIM SM) e IGMP (Internet Group Management Protocol) almeno versioni v2 e v3. Nel caso di utilizzo del protocollo IPv6 il fornitore dovrà utilizzare il protocollo Multicast Listener Discovery (MLD) v1 e v2 descritto nelle RFC 3810 e 4604.

[R.64] Il fornitore dovrà realizzare un servizio di multicast all'interno della propria rete in grado di trasferire informazioni da sorgenti di flussi multicast di proprietà dell'Amministrazione a più destinatari posti sull'intranet dell'Amministrazione.

[R.65] Il fornitore dovrà gestire l'indirizzamento multicast IPv4 e/o IPv6 della rete necessario per fornire il servizio alle Amministrazioni.

4.5 Opzione dei servizi di trasporto dati: Estensione apparato Wi-Fi

[RR.51] L'opzione Estensione apparato Wi-Fi prevede l'attivazione di una funzionalità di accesso senza fili in ambito privato (indoor). La funzionalità deve supportare almeno i seguenti standard:

- IEEE 802.11b/g/n;
- IEEE 802.11i (WPA2).

4.6 Servizi accessori di Backup

[RR.52] Il servizio accessorio (e quindi facoltativo) di Backup offre una funzionalità di ridondanza basata su tecnologia differente rispetto a quella caratterizzante il servizio base, ma non include alcuna garanzia di eventuale SBRI presente sull'accesso primario. Il servizio accessorio prevede l'utilizzo di tre possibili tecnologie:

- **backup ISDN**: il servizio di backup è implementato tramite un accesso BRI (2 canali a 64 kbps) per ciascun singolo servizio di accesso contrattualizzato. Il servizio si intende comprensivo di tutte le dotazioni tecnologiche necessarie alla soluzione, dei canoni e dell'eventuale traffico associati alla linea ISDN;
- **backup Radiomobile**: il servizio di backup è implementato tramite apparati che consentono il trasporto di dati su rete radiomobile. Il servizio prevede la fornitura e l'utilizzo di SIM (Subscriber Identification Module) in grado di gestire traffico EDGE/UMTS/HSDPA/LTE (o evoluzioni). Il servizio si intende comprensivo di tutte le dotazioni tecnologiche necessarie alla soluzione, dei canoni e dell'eventuale traffico associati alla SIM radiomobile;
- **backup Satellitare**: il servizio di backup è implementato tramite apparati che consentono il trasporto di dati su rete satellitare. Le caratteristiche del servizio sono definite nei requisiti [RR.55], [RR.56], [RR.57], [RR.58] e [RR.59].

[RR.53] Il servizio accessorio di Backup prevede attività di monitoraggio e gestione tali da rilevare eventuali malfunzionamenti anche in condizioni di normale operatività dell'accesso primario ed è comprensiva di tutte le funzionalità/apparati necessari al re-indirizzamento del traffico sul link di backup in caso di indisponibilità del collegamento primario o, nel caso di servizi in alta affidabilità, in condizioni di indisponibilità sia del collegamento primario che del secondario. Il servizio accessorio deve prevedere anche tutte le funzionalità necessarie al re-indirizzamento del traffico sul link primario non appena questo venga correttamente ripristinato. Considerando che il collegamento di backup deve essere inattivo in caso di disponibilità del servizio primario, il servizio accessorio non prevede l'implementazione di politiche di load balancing.

[RR.54] Il PAS del servizio accessorio di Backup coincide con il PAS del servizio di accesso primario associato.

[RR.55] Il servizio backup satellitare prevede l'utilizzo di un collegamento satellitare bidirezionale asimmetrico, con le caratteristiche di banda in Downlink e in Uplink indicate nella seguente tabella:

Profilo	BNA (Down/Uplink)	
STBS-1	20 Mbpsec	6 Mbpsec
STBS-2	6 Mbpsec	6 Mbpsec

[RR.56] Il servizio backup satellitare si intende comprensivo di tutte le dotazioni tecnologiche necessarie alla soluzione (collegamento fra il satellite e l'Amministrazione, collegamento fra il satellite e la rete del Fornitore, parabole e cablaggi necessari per la fruizione del servizio fino ad un massimo di 50 metri, apparato di attestazione in sede dell'Amministrazione).

[RR.57] I servizi di back-up satellitare devono rendere disponibili, la componente di traffico caratterizzata da velocità di picco con throughput fino all'intero valore di BNA definito per il singolo accesso, banda minima garantita down/up con e per un volume di traffico incluso nel canone mensile pari a quanto indicato in [RR.58] in termini di GByte/anno (download + upload).

[RR.58] Al fine di considerare il servizio disponibile, la banda messa a disposizione per ogni singolo accesso non deve essere mai inferiore ai valori di Banda minima garantita prevista per ogni servizio STBS 1 STBS 2 all'interno della soglia di volume di traffico in Giga Byte stimato su base annuale. Al superamento di una soglia di traffico in trasmissione e ricezione, la banda disponibile in modalità Best Effort può essere ridotta al valore BBE riportata in tabella. L'intera disponibilità della BNA deve essere ripristinata al termine del periodo di riferimento.

Profilo	BNA		BGA		Volume di traffico annuale	BBE (Down/ Uplink in Kbps)	
	(Down/ Uplink in Mbps)		(Down/Uplink in Kbps)		GB		
STBS-1	20	6	64	32	40	256	128
STBS-2	6	6	256	256	150	512	512

[RR.59] Il servizio di back-up deve inoltre prevedere una gestione proattiva di *Problem Management*, mediante l'uso di sistemi di monitoraggio da remoto delle funzionalità del terminale satellitare, atta a prevenire eventuali indisponibilità della linea in caso di necessità di utilizzo della linea di back-up.

4.6.1 Opzioni del servizio accessorio di Backup

[RR.60] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio accessorio Backup tramite ISDN o radiomobile o rete satellitare:

- Finestra di erogazione estesa (cfr. [R.6]), col vincolo che la finestra di erogazione del servizio accessorio di Backup coincida con quella del servizio di accesso primario associato.

5 SERVIZIO DI POSTA ELETTRONICA (SPE)

Il servizio di posta elettronica consente al personale dell'Amministrazione di comunicare attraverso messaggi asincroni creati, spediti e ricevuti in formato elettronico da postazioni di lavoro individuali sia con l'interno che con l'esterno dell'Amministrazione.

[RR.61] Il servizio di posta elettronica è facoltative.

[RR.62] Il servizio di posta elettronica deve essere erogato su un'infrastruttura/piattaforma centralizzata dedicata alle Amministrazioni della CN RUPAR-SPC dislocata presso il Centro Servizi del Fornitore.

[RR.63] Il servizio deve assumere come riferimento lo standard SMTP (RFC2821) per la messaggistica di tipo testuale, lo standard ESMTP/MIME (RFC2821/RFC2045, RFC2046, RFC2047, RFC2048, RFC2049) per lo scambio di messaggi non solo testuali.

[RR.64] Il Fornitore deve erogare un servizio di posta elettronica caratterizzato dalle seguenti funzionalità:

- controllo antivirus sui messaggi scambiati e sui loro allegati attivabile e disattivabile su richiesta;
- assegnazione e gestione degli account di posta nello spazio di naming concordato con le Amministrazioni;
- accesso da parte di ciascun utente alla propria casella di posta solo previo riconoscimento delle credenziali dell'utente (*userid* e *password*);
- accesso alle caselle attraverso i protocolli SMTP, POPv3, IMAP;
- accesso alle caselle attraverso il supporto di protocolli sicuri basati su SSL/TLS come ad esempio POPS e IMAPS;
- accesso alle caselle attraverso protocollo HTTP, HTTPS ed interfaccia Web;
- le sessioni di invio della posta devono prevedere obbligatoriamente la verifica dell'account di posta dell'utente e la sua coincidenza con l'indirizzo mittente della mail (invio controllato mediante autenticazione);
- le sessioni di invio e ricezione della posta devono prevedere almeno la crittografia della password di autenticazione.

[RR.65] Il Fornitore deve assicurare la continuità del servizio di posta elettronica prevedendo adeguati meccanismi di "backup a caldo" che evitino perdite di informazioni scambiate.

[RR.66] Il servizio SPE prevede esclusivamente l'adozione di una finestra di erogazione estesa H24 in sostituzione della finestra di erogazione standard (cfr. [R.6]).

[RR.67] Il Fornitore deve fornire a ciascuna Amministrazione quantità di spazio su disco remoto con granularità di 10 MByte ed attivare successivamente il numero richiesto di caselle di posta con il vincolo di prevedere almeno 10 MByte a casella per la memorizzazione dei messaggi e di altri dati inseriti dall'utente.

[RR.68] Il Fornitore deve prevedere la possibilità di:

- ridistribuire lo spazio su disco remoto senza oneri tra le caselle già acquistate dall'Amministrazione;
- incrementare lo spazio su disco remoto mediante la fornitura di spazio aggiuntivo qualora l'Amministrazione ne faccia richiesta;
- attivare nuove caselle di posta senza alcun onere qualora l'Amministrazione decida di non utilizzare nuovo spazio su disco remoto, ma di ridistribuire quello già presente, purché sia rispettato il vincolo di dimensione minima della casella di 10 MByte.

[RR.69] Fatto salvo lo spazio disponibile sulla casella, non dovrà essere previsto un limite alla dimensione massima dei messaggi scambiati né degli eventuali allegati in essi contenuti.

[RR.70] Il Fornitore deve rendere disponibile all'Amministrazione un servizio accessibile da personale autorizzato dell'amministrazione tramite browser Web, che consenta la modifica dei parametri di configurazione del servizio (creazione di nuove caselle, variazione delle dimensioni delle caselle).

[RR.71] Oltre alle funzionalità di base di invio, inoltro, risposta e cancellazione di un messaggio, su ciascuna casella, anche da Web, il fornitore dovrà rendere disponibili le seguenti funzionalità aggiuntive:

- risposta automatica ai messaggi in funzione di parametri configurabili;
- inoltro automatico di messaggi in funzione di parametri configurabili;
- costruzione di liste di distribuzione;
- regole di gestione automatica di posta in arrivo;
- strumenti di antispamming;
- almeno tre indirizzi di alias.

6 SERVIZI DI SICUREZZA

Il Fornitore deve erogare i Servizi di Sicurezza descritti dal presente capitolato in modo da:

- proteggere il sistema informativo e la relativa infrastruttura tecnologica sotto il dominio amministrativo delle Amministrazioni;
- proteggere le infrastrutture telematiche interconnesse con tali servizi.

I servizi di sicurezza richiesti dal presente capitolato si caratterizzano come servizi di sicurezza perimetrale, volti a fornire prestazioni per il controllo di sicurezza del traffico relativo agli accessi alla CN RUPAR-SPC e alle reti della PA ad esso collegate. Tali servizi si articolano in:

- Servizi di sicurezza perimetrale unificata (SPUN) cfr. § 6.1.1;
- Servizi di sicurezza Centralizzata (SCEN) cfr. § 6.1.2;

[R.87] Le soluzioni e i servizi proposti dal Fornitore devono essere:

- aggiornati dal punto di vista tecnologico, con riferimento all'evoluzione degli standard e del mercato;
- conformi alle normative e agli standard di riferimento applicabili;
- adeguati in modo continuativo alle normative che la Comunità Europea o l'Italia rilasceranno in merito a servizi analoghi a quelli descritti nel presente Documento senza oneri aggiuntivi per le Amministrazioni.

[R.88] I servizi descritti nel presente capitolato si intendono comprensivi di tutte le componenti HW e SW necessarie ai fini dell'erogazione degli stessi.

[RR.72] Il Fornitore deve erogare i servizi di sicurezza utilizzando apparati che si raccordino con i sistemi dell'Amministrazione attraverso interfacce conformi agli standard IEEE Fast-Ethernet 10/100 Autosensing, Gigabit-Ethernet o 10 Gigabit Ethernet. Limitatamente alle interfacce disponibili sul profilo di Firewall richiesto, è facoltà dell'Amministrazione scegliere fra le interfacce indicate sopra.

[RR.73] Gli apparati utilizzati devono supportare funzionalità di routing statico e routing dinamico (almeno i protocolli RIP e OSPF).

[R.90] Il Fornitore ha la completa responsabilità della configurazione, gestione, monitoraggio e manutenzione delle componenti che realizzano i servizi di sicurezza perimetrale. L'Amministrazione ha comunque la responsabilità di esprimere al Fornitore tutti i requisiti necessari per la corretta installazione e configurazione dei servizi e fornire tutte le informazioni di propria competenza.

[RR.74] Tutti i servizi di sicurezza devono essere erogati dal Fornitore in modalità di "outsourcing completo", mediante l'attivazione di un Centro di Gestione per la Sicurezza (SOC – Security Operating Center), non necessariamente dedicato ai servizi della CN RUPAR-SPC, che ha il compito di gestire le risorse utilizzate per erogare i servizi di sicurezza.

[R.92] Gli apparati collocati presso sedi delle Amministrazioni ed utilizzati per erogare i servizi di sicurezza perimetrale devono essere dotati di funzionalità di gestione remota tramite protocolli cifrati.

[R.93] Tutti i dispositivi utilizzati per l'erogazione dei servizi di sicurezza devono implementare meccanismi di Identificazione, Autenticazione, Autorizzazione e Accounting (IAAA) attraverso i quali sia possibile l'accesso logico da console e da remoto per attività di gestione e/o di Amministrazione.

[R.94] Per l'autenticazione possono essere supportati uno o più meccanismi tra quelli riportati di seguito:

- Accesso da console:

- Server Radius;
- Password statiche configurabili sul dispositivo utilizzato;
- Password dinamiche generate per il tramite di token;
- One Time Password (OTP).

- Accesso da remoto:
  - Password dinamiche generate per il tramite di token;
  - One Time Password (OTP).

Il Fornitore può proporre in alternativa un diverso schema di autenticazione, che deve essere approvato in fase di collaudo del servizio, purché la comunicazione tra la stazione di gestione e l'apparato gestito sia protetta dall'uso di un adeguato algoritmo crittografico.

[R.95] I sistemi adottati devono rilevare e registrare i tentativi di accesso non autorizzato al sistema stesso.

[R.96] Per quanto riguarda le attività di gestione e Amministrazione, i sistemi devono essere in grado di generare log di audit contenenti almeno le seguenti informazioni: data, ora evento, identità del soggetto, successo/fallimento dell'evento.

[RR.75] I dati registrati dal sistema di sicurezza devono essere disponibili per l'uso da parte degli utenti abilitati ovvero gli amministratori del servizio (personale del Fornitore), i soggetti indicati dall'Amministrazione e i soggetti autorizzati per legge.

[R.98] I file di log devono essere protetti da modifiche o cancellazioni non autorizzate, in conformità alla normativa vigente.

[R.99] I dispositivi utilizzati devono garantire la piena compatibilità IPv6 e il supporto di base dual stack Firewall (IPv4 e IPv6) e dei protocolli IPv4 e IPv6 subordinati.

[R.100] I sistemi adottati devono essere in grado di risolvere problematiche di NAT/Firewall traversal per i protocolli VoIP.

6.1 Servizi di Sicurezza Perimetrale

6.1.1 Servizio di Sicurezza Perimetrale Unificata (SPUN)

[R.101] Il servizio di Sicurezza Perimetrale Unificata deve prevedere elementi architetturali atti a implementare le seguenti funzionalità di base:

- Firewall;
- VPN IPsec Site-to-Site;
- Intrusion Detection & Prevention System (IDS/IPS).

[RR.76] I servizi SPUN sono disponibili in sei distinte modalità di erogazione del servizio (differenti profili di servizio contrattualizzabili dall'Amministrazione). Tali profili si differenziano in base a:

- **coppia di parametri Firewall e IPS Throughput**: rappresentano il throughput minimo che deve essere rispettivamente gestito dalle due prestazioni del servizio;
- **massimo numero di Tunnel VPN IPsec S2S simultanei**: rappresenta il numero massimo di tunnel VPN IPsec Site-to-Site simultanei che l'apparato di sicurezza è in grado di gestire.

[RR.77] I diversi profili previsti per il servizio SPUN sono caratterizzati dai requisiti riportati nella presente tabella:

Profilo	Firewall Throughput (Mbps)	IPS Throughput (Mbps)	Tunnel VPN IPsec S2S simultanei

SPUN-1	100	40	10
SPUN-2	200	100	20
SPUN-3	450	200	50
SPUN-4	1.500	650	100
SPUN-5	4.000	2.000	500
SPUN-6	20.000	8.000	1.000

[RR.78] Il Fornitore, quando è chiamato a modificare e/o aggiornare le politiche di sicurezza (operazioni di Change Management) sulla base di esigenze espresse dall'Amministrazione, è tenuto a eseguire le richieste pervenute per un numero illimitato di volte. Tuttavia:

- sono soggette a SLA solo le operazioni che rientrano nel limite fissato dallo specifico profilo associato al servizio SPUN indicate nella seguente tabella

Profilo	Change management (interventi annuali)
SPUN-1	20
SPUN-2	25
SPUN-3	30
SPUN-4	35
SPUN-5	40
SPUN-6	45

- oltre tale limite, le operazioni non saranno più soggette a SLA ma devono essere garantite dal Fornitore e gestite in modalità Best Effort.

[R.105] Le funzionalità del servizio base indicate in [R.101], e le eventuali funzionalità opzionali acquistate dalle Amministrazioni (cfr. § 6.1.1.4 e specificamente [R.130]), devono essere erogate attraverso l'utilizzo di un unico dispositivo HW, configurato in modo tale da rispettare le caratteristiche tecniche e prestazionali descritte nel presente Capitolato ed i livelli di servizio definiti nell'Allegato 1.1 - Livelli di servizio e penali.

[R.106] Gli apparati devono essere dotati di almeno n° 3 interfacce di tipo Fast-Ethernet 10/100 Autosensing, Gigabit-Ethernet o 10 Gigabit Ethernet. Per ciascun servizio SPUN la somma della capacità delle interfacce non deve essere inferiore al Firewall Throughput indicato nella tabella del [RR.77] per lo SPUN corrispondente.

[R.107] Alcune delle funzionalità offerte dal servizio di sicurezza si basano su "signature", che devono essere aggiornate entro, e non oltre, 1 giorno dal momento in cui sono rese disponibili dal vendor che fornisce i sistemi utilizzati dal Fornitore per l'erogazione del servizio di sicurezza.

[R.108] Il Punto di accesso al servizio (PAS) per i servizi SPUN è definito come l'insieme delle interfacce messe a disposizione sul dispositivo HW di cui al [R.105].

6.1.1.1 Funzionalità SPUN: Firewall

[RR.79] Il servizio deve essere dotato di una funzionalità di firewalling che permetta di analizzare tutti i flussi di traffico a differenti livelli della pila ISO/OSI, bloccando quelli che appartengono a collegamenti non autorizzati tramite almeno funzionalità "stateful inspection", secondo le regole configurate dal Fornitore sulla base delle esigenze espresse dall'Amministrazione.

[R.110] Il sistema di firewalling su cui è basato il servizio deve supportare tutti i protocolli specificati nello standard TCP/IP.

[RR.80] La funzionalità di firewalling deve implementare le seguenti caratteristiche di base:

- filtraggio di traffico IP che consente di proteggere una rete IP da accessi indesiderati bloccando indirizzi, porte o protocolli;
- auditing e logging che consente l'analisi del traffico che attraversa il firewall;
- modulo di ispezione che effettua l'ispezione dei datagrammi IP e realizza il filtraggio sulla base delle regole implementate. Deve essere implementata almeno la metodologia "stateful inspection" escludendo l'impiego di dispositivi di firewalling di tipo Packet Filtering Stateless;
- modulo di gestione che consente di configurare e monitorare il comportamento del sistema firewall;
- meccanismi antispoofing;
- meccanismi di rilevazione e protezione per attacchi di tipo Denial of Service;
- Network Address Translation (NAT) secondo la specifica RFC 3022, sia di tipo statico (uno a uno), sia di tipo dinamico (n a uno) e Port Address Translation (PAT);
- URL filtering che consente solo a determinate postazioni di abilitare la navigazione Web attraverso il firewall, di controllare le statistiche sulla navigazione e di bloccare l'accesso a particolari siti Internet/Intranet; le modalità di individuazione dei siti sono *DNS Name*, indirizzo IP o dominio;
- Web Content Filtering che consente di filtrare dinamicamente il contenuto delle pagine web bloccando l'accesso a contenuti ritenuti inopportuni.

6.1.1.2 Funzionalità SPUN: VPN IPsec Site-to-Site

[R.112] Il servizio deve comprendere la funzionalità di realizzazione di reti private virtuali basate sullo standard IPsec come definito dall'IPsec Working Group dell'IETF (RFC 4301).

[R.113] La funzionalità di VPN IPsec Site-to-Site deve implementare le seguenti caratteristiche:

- *Data origin authentication* che verifica l'autenticità del mittente di ciascun datagramma IP;
- *Data integrity* che verifica che il contenuto di ciascun datagramma non sia stato modificato (deliberatamente o a causa di errori di linea) durante il transito tra sorgente e destinazione;
- *Data confidentiality* che nasconde il testo in chiaro contenuto in un messaggio, mediante l'impiego della crittografia;
- *Replay protection* che assicura che una terza parte non autorizzata, intercettato un datagramma IP, non sia in grado, a posteriori, di rispedirlo a destinazione per qualche scopo illecito.

[R.114] Il servizio deve prevedere il supporto per IPsec "Tunnel mode" e "Transport mode" come definiti nella specifica pubblica RFC 4301.

[R.115] Nell'implementazione e nella gestione delle reti private virtuali, il Fornitore deve erogare il servizio secondo una delle seguenti modalità:

- **Autonoma**: il Fornitore deve provvedere alla realizzazione e gestione di entrambe le terminazioni dei tunnel che realizzano la VPN dell'Amministrazione;
- **Cooperativa**: il Fornitore deve interagire con altri Fornitori per la realizzazione e gestione dei tunnel che realizzano la VPN. Quest'ultimo caso si riferisce a tutti quegli scenari secondo i

quali il dispositivo che realizza un'estremità di un tunnel risulta sotto il dominio amministrativo di un Fornitore diverso da quello che amministra l'altra estremità;

- **Predefinita**: ai fini di semplificare la gestione cooperativa nei casi in cui differenze tecnologiche e gestionali tra Fornitori diversi non garantiscano una completa interoperabilità, è possibile che la scelta del Fornitore sia dettata dall'Amministrazione che eroga i servizi applicativi. Le altre Amministrazioni, per poter usufruire dei servizi su VPN IPsec, devono richiedere tale servizio allo stesso Fornitore. È pertanto responsabilità del Fornitore la progettazione e la fornitura del servizio.

[R.116] Il Fornitore è completamente responsabile dell'erogazione dei servizi in modalità autonoma o predefinita, mentre il servizio, erogato in modalità cooperativa, richiede l'implementazione e la gestione dell'estremità dei tunnel sotto il dominio amministrativo del Fornitore, oltre a tutte le attività necessarie per attivare il tunnel con Fornitori terzi che gestiscono l'altra estremità. La modalità cooperativa richiede che il Fornitore impieghi sistemi interoperabili con terminazioni di tunnel diverse, gestite da Fornitori terzi.

[R.117] Relativamente all'autenticazione dei nodi e alla gestione delle associazioni di sicurezza, la creazione e la negoziazione delle associazioni di sicurezza (SA, Security Association) del sistema IPsec devono essere garantite attraverso i meccanismi identificati dal protocollo Internet Key Exchange (IKE) secondo la specifica pubblica RFC 5996. Tali meccanismi devono supportare sia l'autenticazione mediante segreto condiviso ("*pre-shared key*") che quella mediante certificati digitali conformi allo standard ISO/IES 9594-8 (X.509v3).

[RR.81] In particolare, l'impiego dei certificati digitali è obbligatorio qualora il servizio sia erogato in modalità cooperativa; ogni fornitore provvede ad approvvigionare i certificati digitali per la terminazione di propria competenza.

[RR.82] Il Fornitore si impegna ad erogare il servizio VPN IPsec utilizzando certificati digitali X.509v3. Per quanto concerne le VPN di tipologia Cooperativa i certificati devono essere emessi esclusivamente da una Certification Authority di rete situata sul territorio italiano; per le VPN di tipologia Autonoma e Cooperativa i certificati devono essere emessi o da una Certification Authority di rete situata sul territorio italiano o da una CA interna privata del Fornitore.

[R.120] Il formato per le richieste dei certificati deve essere conforme allo standard PKCS#10.

[R.121] Il servizio deve prevedere l'adozione di adeguati meccanismi di protezione della chiave privata e delle chiavi di sessione memorizzate nei dispositivi utilizzati.

[R.122] Prima dell'apertura di un nuovo tunnel crittografico, deve essere verificato lo stato di validità del certificato con l'ausilio delle Certification Revocation List (CRL) o, in alternativa e preferibilmente, direttamente online con il supporto del protocollo OCSP.

6.1.1.3 Funzionalità SPUN: Intrusion Detection & Prevention System (IDS/IPS)

[R.123] Il servizio prevede la funzionalità di rilevamento e prevenzione delle intrusioni che consenta di identificare (IDS) e, laddove possibile, interrompere (IPS) azioni aventi come obiettivo la violazione o la compromissione del funzionamento di un sistema, di un apparato o di una rete.

[R.124] Per il riconoscimento dei potenziali attacchi, il servizio erogato dal Fornitore deve utilizzare informazioni presenti in una banca dati centrale costantemente aggiornata e compatibile con le Common Vulnerabilities and Exposures (CVE-compatible).

[RR.83] Il sistema deve prevedere una raccolta e conservazione delle tracce tipiche di un determinato attacco, allo scopo di favorire l'individuazione degli autori dell'attacco, per un periodo compatibile con i tempi minimi previsti dalla normativa vigente.

[R.126] Il sistema deve prevedere meccanismi di notifica a fronte dell'identificazione di un evento di attacco.

[R.127] Il servizio di Intrusion Detection & Prevention deve prevedere almeno le seguenti tecniche di rilevazione degli attacchi:

- Anomalia di traffico/protocollo: analisi dei flussi di traffico ed individuazione di anomalie nei protocolli comunemente utilizzati nell'ambito delle reti IP;
- "Signature analysis": analisi basata su signature che consente di riconoscere le serie di pacchetti (o i dati contenuti in essi), selezionate preventivamente in fase di configurazione al fine di riconoscere un tipico pattern rappresentativo di un attacco.

[R.128] Il servizio fornito deve disporre di una struttura in grado di rilasciare aggiornamenti delle signature utilizzate per il rilevamento degli attacchi. Il sistema deve quindi essere in grado di aggiornare le signature automaticamente, senza l'intervento manuale dell'operatore.

[R.129] In caso di rilevamento di un attacco, il sistema deve essere in grado di impedirne l'esecuzione per mezzo delle seguenti tecniche di prevenzione:

- Drop packet/session, ossia scarto del pacchetto/sessione;
- Close client/server, ossia invio di un segnale di chiusura (reset) lato client e/o server.

6.1.1.4 Opzioni del servizio SPUN

[R.130] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio di Sicurezza Perimetrale Unificata:

- **Affidabilità elevata** (cfr. [RR.85]);
- **Antivirus/Antispyware & Content filtering** (cfr. da [R.133] a [R.138] e da [RR.86] e [RR.88]);
- **Application filtering and monitoring** (cfr. da [R.142] a [R.146]);
- **Accesso remoto sicuro (VPN Client-to-site)** (cfr. da [R.147] a [R.152] e [RR.89]);
- **Finestra di erogazione estesa** (cfr. [R.6]).

[RR.84] Le funzionalità incluse in questa opzione possono essere implementate utilizzando lo stesso dispositivo utilizzato per l'erogazione del servizio SPUN (o gli stessi dispositivi se è attivata l'opzione di Affidabilità elevata).

[RR.85] L'opzione **Affidabilità elevata** prevede, a fronte della corresponsione di un canone aggiuntivo, la duplicazione dell'apparato fornito per l'erogazione dei servizi di sicurezza, gestiti e manutenuti dal Fornitore. L'apparato aggiuntivo deve essere installato nel medesimo locale tecnico ove è installato l'apparato primario. Il servizio prevede la configurazione in "hot-standby" degli apparati primario e secondario, e quindi la possibilità di mantenimento trasparente delle funzioni di sicurezza in caso di guasto. Gli apparati forniti devono essere bi-attestati agli apparati di rete utilizzati per lo scambio del traffico tra la rete da proteggere e l'esterno. Gli SLA del servizio per quanto riguarda i parametri di assurance sono differenziati rispetto al servizio base (cfr. Allegato 1.1 - Livelli di servizio e penali).

[R.133] L'opzione **Antivirus/Antispyware & Content Filtering** deve attivare funzionalità in grado di proteggere il Sistema Informativo delle Amministrazioni da spamming, da attacchi veicolati tramite il protocollo HTTP e da codice eseguibile (Virus, Spyware, Worm, Cavallo di Troia, ecc.).

[R.134] Il Fornitore deve garantire le seguenti caratteristiche per tali funzionalità:

- Antivirus/Antispyware Gateway (AVG) per la protezione da codice dannoso che può propagarsi tramite lo scambio di posta elettronica;
- HTTP Gateway (HTTPG) per la protezione da codice dannoso che può propagarsi per il tramite della navigazione WEB e per la protezione da attacchi informatici veicolati tramite il protocollo http;
- FTP Gateway (FTPG) per la protezione da codice dannoso che può propagarsi per il tramite del trasferimento di file mediante FTP;

[R.135] La soluzione proposta deve garantire la rilevazione dei virus e degli spyware noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e dal formato di trasmissione.

[R.136] La soluzione proposta deve garantire la capacità di scansione dei pacchetti IP in tempo reale.

[R.137] La soluzione proposta deve garantire piena interoperabilità e/o trasparenza tra client e server.

[R.138] La soluzione proposta deve prevedere il supporto di file in formati compressi per il controllo della presenza di codice dannoso.

[RR.86] La soluzione proposta deve prevedere il supporto dei protocolli standard tipici del servizio (SMTP, POP v.3, IMAP v.4, HTTP, FTP, *Instant Messaging Protocol*).

[RR.87] Per quanto riguarda le caratteristiche di AVG, HTTPG e FTPG il servizio fornito dal Fornitore deve garantire il supporto dei filtri di esclusione sul tipo di file trasferito (vbs, exe, pif, bat, ecc.), indipendentemente dal fatto che contengano malware.

[RR.88] Per quanto riguarda le caratteristiche di AVG, il Fornitore deve garantire le seguenti ulteriori funzionalità:

- supporto di blacklist (liste contenenti domini di mail o indirizzi di mail indesiderati);
- configurazioni antispamming che consentano il blocco di messaggi di posta elettronica che transitano per il gateway basati su blacklist e riconoscimento di porzioni del contenuto del messaggio di posta elettronica personalizzabili;
- verifica sintattica e semantica sull'header dei messaggi.

[R.142] L'opzione **Application Filtering & Monitoring** deve fornire una funzionalità che permetta di effettuare un'analisi delle applicazioni che generano traffico sulla rete, assieme alla possibilità di controllare tali applicazioni, indipendentemente dalla porta e dal protocollo utilizzati dall'applicazione stessa.

[R.143] La funzionalità deve utilizzare un processo per l'analisi del traffico basato su identificativi delle applicazioni e signature.

[R.144] Per le applicazioni che non possono essere identificate attraverso analisi del protocollo e l'adozione delle signature, devono essere previsti meccanismi basati su euristiche e analisi comportamentale.

[R.145] La funzionalità deve essere in grado di applicare politiche basate sull'identità degli utenti, consentendo o negando l'uso di tali applicazioni sulla base del profilo dell'utente o di gruppi di utenti.

[R.146] In particolare, il sistema deve essere in grado di bloccare, e laddove possibile limitare, la banda utilizzabile e il traffico relativo alle applicazioni selezionate sulla base di politiche impostate secondo i requisiti dichiarati dalle Amministrazioni.

[R.147] L'opzione **Accesso remoto sicuro (VPN Client-to-site IPsec/SSL)** deve prevedere una funzionalità che consenta, al personale delle Amministrazioni, di accedere da remoto alla Intranet attraverso l'utilizzo di postazioni di lavoro mobili (PC, laptop, smartphone, ecc.) in modalità VPN client-to-site IPsec e/o SSL.

[R.148] L'opzione deve operare creando un tunnel tra il nodo interessato e un gateway della rete, utilizzando il protocollo IPsec o in alternativa il protocollo SSL, in base alle esigenze delle Amministrazioni.

[RR.89] Nel caso di utilizzo del protocollo IPsec, il sistema deve operare secondo la modalità "tunnel mode" come definita nella specifica pubblica RFC 4301. In tal caso la parte client deve essere fornita almeno per le seguenti piattaforme: Windows, Linux, Mac; la fornitura dei client IPsec non comprende l'installazione e/o la configurazione dei client stessi.

[R.150] Nel caso dell'utilizzo del protocollo IPsec, devono essere rispettate le specifiche indicate dal [R.117] al [R.122], [RR.81] e [RR.82].

[R.151] Nel caso di utilizzo del protocollo SSL, il sistema deve operare seguendo la specifica pubblica RFC 6101, in modalità *clientless*. In tal caso, gli utenti accedono alla Intranet attraverso un portale web accessibile a valle di un'autenticazione dell'utente. Tale portale web deve quindi fungere da proxy verso un set di applicazioni prestabilito.

[R.152] Il sistema deve essere in grado di supportare un numero di collegamenti in contemporanea a seconda del profilo SPUN di base come riportato nella seguente tabella:

Profilo	Numero massimo di tunnel IPsec simultanei (Client to Site)	Numero massimo di tunnel SSL simultanei (Client to Site)
SPUN-1	10	5
SPUN-2	20	10
SPUN-3	50	25
SPUN-4	100	50
SPUN-5	500	100
SPUN-6	1000	100

6.1.1.5 Precondizioni e vincoli per la sottoscrizione del servizio SPUN

[RR.90] Solo le Amministrazioni che hanno sottoscritto, in ambito CN RUPAR-SPC, servizi di trasporto possono richiedere i servizi SPUN qui descritti e limitatamente alle sedi collegate coi suddetti servizi.

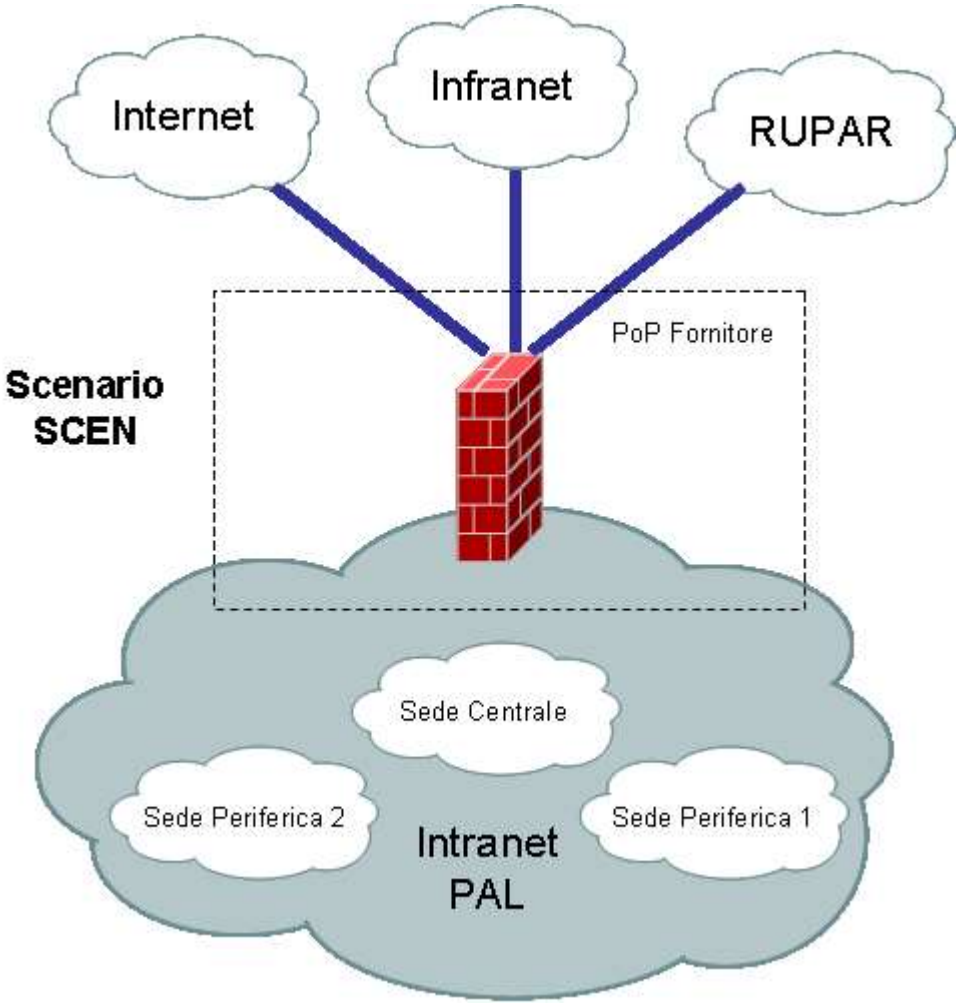
6.1.2 Servizio di Sicurezza Centralizzata (SCEN)

[RR.91] Il **servizio di Sicurezza Centralizzata (SCEN**) prevede l'erogazione di servizi di sicurezza perimetrali (firewall, antivirus, Intrusion Detection/Prevention System) in modalità centralizzata su specifici accessi STDE, STDS, STDW e STDH (limitatamente ai profili da STDH-1 a STDH-3) dell'Amministrazione. Il servizio di sicurezza centralizzato è erogato da un centro servizi del Fornitore locato presso siti del Fornitore medesimo, e deve essere adeguatamente dimensionato per far fronte al carico complessivo generato da tutti i servizi contrattualizzati da tutte le Amministrazioni nel perimetro di competenza del Fornitore.

[RR.92] Il Fornitore, quando è chiamato a modificare e/o aggiornare le politiche di sicurezza (operazioni di Change Management) sulla base di esigenze espresse dall'Amministrazione, è tenuto a eseguire le richieste pervenute per un numero illimitato di volte. Tuttavia:

- sono soggette a SLA solo 20 operazioni;
- oltre tale limite, le operazioni non saranno più soggette a SLA ma devono essere garantite dal Fornitore e gestite in modalità Best Effort.

[RR.93] Il servizio SCEN deve essere collocato alla frontiera tra il dominio Intranet ed i domini RUPAR, Infranet ed Internet, e quindi eventualmente esposto su indirizzi privati dell'Amministrazione, secondo quanto riportato nella figura seguente:



[RR.94] Il servizio SCEN comprende una componente di network firewall in grado di offrire protezione per il tramite di analisi e filtro di tutto il traffico in transito tra le reti tra cui è interposto, con le seguenti caratteristiche:

- supporto di tutti i protocolli specificati nello standard TCP/IP;
- filtraggio di traffico IP che consente di proteggere la rete dell'Amministrazione da accessi indesiderati bloccando indirizzi, porte o protocolli;
- auditing e logging che consente l'analisi del traffico che attraversa il servizio;
- modulo di ispezione che effettua l'ispezione dei datagrammi IP e realizza il filtraggio sulla base delle regole implementate;
- Traffic Filtering, che consenta di abilitare la navigazione web (ambito Internet) solo a determinate postazioni (intese come indirizzi IP di provenienza), e di bloccare l'accesso a particolari siti; le modalità di individuazione dei siti sono *DNS Name*, indirizzo IP o dominio;
- Network Address Translation (NAT) secondo la specifica RFC 3022, sia di tipo statico (uno a uno), sia di tipo dinamico (n a uno) e Port Address Translation (PAT);
- Web Content Filtering che consente di filtrare dinamicamente il contenuto delle pagine web bloccando l'accesso a contenuti ritenuti inopportuni.

[R.157] Il servizio SCEN comprende una componente di Antivirus Filtering in grado di garantire protezione agli accessi dell'Amministrazione nei confronti di spamming, attacchi veicolati tramite il protocollo HTTP e da qualsiasi tipologia di codice software eseguibile (Virus, Worm, Cavallo di Troia, ecc.) che possa provocare danni al Sistema Informativo dell'Amministrazione. Tale

servizio di gestione centralizzata delle funzionalità antivirus deve offrire protezione da codice dannoso che può propagarsi per il tramite:

- dello scambio di posta elettronica;
- della navigazione web tramite il protocollo HTTP;
- del trasferimento di file mediante protocollo FTP.

[R.158] Il servizio SCEN comprende una componente di Intrusion Detection System (IDS) in grado di effettuare un rilevamento delle intrusioni tale da consentire l'identificazione di tutte le sequenze di eventi, condotti da una o più entità non autorizzate, aventi come obiettivo la compromissione di un sistema, di un apparato o di una rete. Il servizio deve in particolare:

- garantire analisi predeterminate degli eventi rilevati attraverso l'utilizzo di "*signature analysis*" che consentano di riconoscere le serie di pacchetti (o i dati contenuti in essi), selezionate preventivamente in fase di configurazione, al fine di riconoscere un tipico pattern rappresentativo di un attacco;
- garantire notifiche specifiche a fronte dell'identificazione di un evento di attacco;
- garantire notifiche all'Amministrazione in merito ad eventuali situazioni che necessitino di interventi/decisioni da parte dell'Amministrazione stessa;
- essere customizzabile in termini di definizione di regole personalizzate, registrazione delle attività sulla rete che rispondano a determinate condizioni, attivazione delle notifiche a fronte di particolari sequenze di eventi sulla rete, ecc.

[R.159] Il servizio SCEN comprende una componente di Intrusion Prevention System (IPS) in grado di svolgere azioni per bloccare selettivamente il traffico in caso di identificazione positiva di tutte le sequenze di eventi, condotte da una o più entità non autorizzate, aventi come obiettivo la compromissione di un sistema, di un apparato o di una rete. Tale caratteristica di IPS deve in particolare garantire funzionalità di:

- analisi di protocollo, al fine di valutare le diverse parti di un protocollo alla ricerca di comportamenti anomali;
- ricerca all'interno dei pacchetti di sequenze uniche per rilevare e prevenire attacchi noti come Worm;
- prevenzione da attacchi di tipo DoS (Denial of Service) e DDoS (Distributed DoS).

[R.160] Alcune delle funzionalità offerte dal servizio di sicurezza si basano su "*signature*", che devono essere aggiornate entro, e non oltre, 1 giorno dal momento in cui sono rese disponibili dal vendor che fornisce i sistemi utilizzati dal Fornitore per l'erogazione del servizio di sicurezza.

[RR.95] Il servizio SCEN deve essere configurato dal Fornitore in modo da garantire che in caso di malfunzionamento della funzionalità di sicurezza, venga inibita completamente la capacità di trasmissione/ricezione del traffico fra l'accesso dell'Amministrazione e gli ambienti Internet e Infranet, mantenendo comunque attiva la comunicazione in ambito Intranet.

[R.162] Il servizio SCEN non è caratterizzato da PAS.

6.1.2.1 Opzioni del servizio SCEN

[RR.96] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio SCEN:

- Finestra di erogazione estesa (cfr. [R.6]), col vincolo che la finestra di erogazione del servizio SCEN coincida con quella del servizio di trasporto associato.

6.1.2.2 Precondizioni e vincoli per la sottoscrizione del servizio SCEN

[RR.97] Un servizio SCEN può essere attivato solo in relazione ad un accesso con opzione Multiambito.

7 SERVIZI DI COMUNICAZIONE EVOLUTA

I Servizi di Comunicazione Evoluta sono dedicati a consentire alle Amministrazioni di effettuare comunicazioni voce o audio/video utilizzando il medesimo accesso attraverso il quale viene approvvigionata la connettività IP (servizi di trasporto).

I Servizi di Comunicazione Evoluta si articolano in

- **Servizi VoIP (VOIP)**: devono consentire alle Amministrazioni contraenti di effettuare conversazioni telefoniche su protocollo IP;
- **Servizi di Telepresenza (TELP)**: devono consentire alle Amministrazioni la comunicazione tra utenti remoti attraverso strumenti di acquisizione/riproduzione audio/video di alta qualità.

[RR.98] I Servizi di Comunicazione Evoluta sono facoltativi.

[R.165] Le soluzioni e i servizi proposti devono essere:

- conformi a direttiva 1999/5/CE (D.Lgs. 9 maggio 2001, n. 269), direttiva 2009/125/CE (D.Lgs. 15 febbraio 2011, n.15), direttiva 2002/95/CE (D. Lgs. 151/2005) e, in generale, completamente conformi alla normativa vigente e agli standard di riferimento applicabili;
- adeguati in modo continuativo alle normative che la Comunità Europea o l'Italia rilasceranno in merito a servizi analoghi a quelli descritti nel presente Documento senza oneri aggiuntivi per le Amministrazioni;
- aggiornati dal punto di vista tecnologico, con riferimento all'evoluzione degli standard e del mercato.

[R.166] Il servizio deve essere garantito nelle modalità di protocollo IPv4, IPv6 o dual stack.

[RR.99] Tutti i dispositivi devono supportare il protocollo SNMP per consentire monitoring in tempo reale e trouble-shoooting. In alternativa, per i telefoni IP è accettabile una soluzione funzionalmente equivalente basata su TR-069.

7.1 SERVIZI VoIP

[R.168] I servizi VoIP, comprendono:

- Servizi di Centralino IP (CEIP)
- Servizi di Resilienza Periferici (RESI)
- Servizi di Gateway (GWTD e GWIP)
- Servizi di Gestione degli Endpoint (ENIP)

[R.169] I servizi VoIP nel seguito descritti devono:

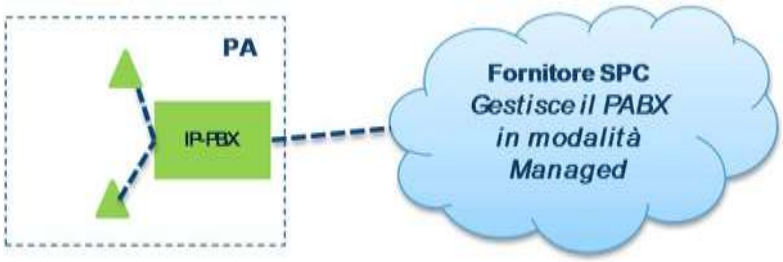
- garantire il rispetto delle disposizioni regolamentari in merito alla interconnessione IP e interoperabilità per la fornitura di servizi VoIP (delibera AGCOM n. 128/11/CIR e smi), in particolare per la definizione di un insieme comune di standard, dei protocolli di segnalazione, dei codec (audio e fax) e funzionalità del VoIP;
- consentire l'invio e la ricezione di fax (con supporto del protocollo T.38).

7.1.1 Servizi di Centralino IP (CEIP)

[RR.100] I servizi CEIP costituiscono il substrato di servizi VoIP disponibile nel listino della CN RUPAR-SPC e rappresentano in tal senso la componente obbligatoria e propedeutica per l'acquisto dei restanti servizi VoIP presenti nel suddetto listino.

[R.172] Il Punto di accesso al servizio (PAS) per i servizi CEIP è definito come l'insieme delle interfacce verso la LAN dell'Amministrazione (e, se disponibili, verso la RTG) sugli apparati che erogano il servizio in sede della Amministrazione.

[R.173] I servizi CEIP sono rivolti a quelle Amministrazioni che non dispongono di infrastrutture di proprietà e consistono nella fornitura, messa in opera, gestione in modalità Managed (on-site) e manutenzione di un'infrastruttura IP-based; prevedono pertanto un apparato IP-PBX presso una sede dell'Amministrazione. Presso le altre sedi dell'Amministrazione il servizio di base non prevede ulteriori apparati; i terminali possono essere acquistati nell'ambito del servizio ENIP di cui al § 7.1.4



[R.174] I servizi devono integrarsi completamente rispetto alle infrastrutture preesistenti, con riferimento alle reti locali delle Amministrazioni e al piano di numerazione dei derivati telefonici che, a richiesta dell'Amministrazione, deve poter essere mantenuto. Quindi all'Amministrazione deve essere garantita la possibilità di:

- riutilizzare numerazioni interne già in uso;
- utilizzare nuove estensioni;
- disporre di un piano di numerazione ex-novo utilizzando una diversa radice.

[R.175] Devono essere erogate funzionalità di gestione della segnalazione per il controllo dei vari stati di una chiamata. Tali funzionalità possono in particolare essere declinate in:

- Incoming Call Gateway: funzione deputata alla gestione della segnalazione al fine del corretto instradamento delle chiamate;
- Call Control Function: funzione deputata all'attivazione, rilascio e gestione/cambiamento degli stati della chiamata, nonché alla determinazione della necessità delle operazioni di transcodifica. Gestisce inoltre la registrazione delle differenti postazioni VoIP ed è in grado di interfacciarsi con server esterni dedicati all'implementazione di servizi a valore aggiunto;
- Serving Profile Database: funzione deputata alla gestione e controllo dei profili delle utenze (es. autorizzazione, abilitazioni, ecc.);
- Address Handling: funzione deputata all'analisi, traduzione, eventuale modifica e risoluzione degli indirizzi da identificativo alfanumerico a indirizzo IP;

Il sistema utilizzato deve supportare il protocollo SIP.

[R.176] Nell'ambito del dominio di una singola Amministrazione (inteso come insieme delle utenze ad essa afferenti), devono essere garantiti almeno i servizi elencati in tabella:

Servizio
Chiamata base
Trasporto dei toni DTMF
Presentazione dell'indirizzo/alias del chiamante
Presentazione del nome del chiamante
Restrizione sulla presentazione del nome del chiamante

Trasferimento incondizionato di chiamata
Trasferimento condizionato di chiamata
Redirezione di chiamata su occupato
Redirezione di chiamata su nessuna risposta
Trattenuta
Parcheggio
Chiamata presa da altro terminale
Richiamata
Conferenza a tre
Autenticazione dell'utente
Indicazione di chiamata in attesa
Musica su attesa
Gestione di suonerie differenziate
Gestione lista chiamate in contemporanea
Sbarramento delle chiamate
Direttore segretaria
Numeri brevi
Rubrica personale e aziendale

[R.177] I servizi CEIP devono prevedere funzionalità di trattamento del segnale audio (echo cancellation).

[RR.101] I servizi CEIP devono garantire funzionalità di autenticazione e autorizzazione nei confronti degli utenti abilitati. Tali funzionalità devono essere implementate per il tramite di comunicazioni logiche IP sicure. A titolo esemplificativo ma non esaustivo, i possibili meccanismi di autenticazione sono: autenticazione basata su MD5 (HTTP Digest) integrata in SIP, Radius, Password dinamiche generate per il tramite di token, One Time Password (OTP), ecc.. Il Fornitore può proporre in alternativa un diverso schema di autenticazione, che deve essere approvato in fase di collaudo del servizio, purché la comunicazione tra la stazione di gestione e l'apparato gestito sia protetta dall'uso di un adeguato algoritmo crittografico.

[R.179] I servizi CEIP devono prevedere funzionalità di *whitelist* e/o *blacklist* sulla base della coppia numero chiamante/numero chiamato.

[R.180] Come detto, l'elemento di gestione della logica di controllo deve essere installato dal Fornitore presso una sede a scelta dell'Amministrazione. Nelle restanti sedi non è prevista l'installazione di alcun apparato, fatta eccezione per gli Endpoint (cfr. § 7.1.4), o gli eventuali apparati previsti dai profili GWTD o GWIP per l'interconnessione a PBX/IP-PBX esistenti (cfr. § 7.1.2). Per quanto detto, in caso di architetture multisede, il prezzo viene sempre calcolato sulla somma di tutte le utenze afferenti alla totalità delle sedi dell'Amministrazione per le quali è stato attivato il servizio.

[R.181] I servizi CEIP sono raggruppati in fasce:

Profilo	Descrizione
CEIP-1	CEIP - 30 utenze
CEIP-2	CEIP - Da 31 a 100 utenze
CEIP-3	CEIP - Da 101 a 300 utenze
CEIP-4	CEIP - Oltre 300 utenze

7.1.1.1 Opzioni dei servizi CEIP

[R.182] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi CEIP:

- **Affidabilità elevata** (cfr. [R.183])
- **Segreteria telefonica** (cfr. [R.184] e [R.185])
- **Finestra di erogazione estesa** (cfr. [R.6])
- **Breakout** (cfr.[RR.102], [R.187] e [R.188])

[R.183] L'opzione **Affidabilità elevata** prevede la duplicazione dell'apparato IP-PBX fornito, gestito e manutenuto dal Fornitore presso la sede dell'Amministrazione. Il secondo IP-PBX deve essere installato nel medesimo locale tecnico ove è installato l'IP-PBX primario. Il servizio prevede la configurazione in hot-standby dell'IP-PBX primario e dell'IP-PBX secondario, l'allineamento continuo e sincrono dei dati di configurazione e delle utenze/terminali gestiti consentendo quindi la possibilità di mantenimento trasparente della chiamata in corso in caso di guasto.

[R.184] L'opzione **Segreteria telefonica** prevede l'erogazione di un servizio di segreteria telefonica agli utenti abilitati; il servizio:

- consiste nella disponibilità di una casella vocale accessibile tramite numerazione ad hoc da un terminale attestato alla centrale telefonica e previa autenticazione;
- deve prevedere la consultazione via accesso remoto (da terminale non attestato alla centrale telefonica) previa autenticazione;
- deve prevedere l'indicazione della data, orario e numero chiamante di ogni chiamata registrata;
- deve garantire uno spazio per utente pari ad almeno 10 minuti di registrazione;
- deve consentire l'integrazione con il sistema di posta elettronica, in uso presso l'Amministrazione (e senza necessità di modifiche di configurazione del sistema mail stesso), per la ricezione di messaggi vocali come normale messaggio di posta con file audio allegato.

[R.185] L'opzione Segreteria telefonica può essere contrattualizzata per un numero di utenze minore o uguale al numero di utenze per le quali è stato contrattualizzato il servizio CEIP.

[RR.102] L'opzione Breakout prevede l'erogazione di un servizio di interfacciamento con la rete telefonica pubblica (breakout) realizzato tramite schede o apparati gateway forniti, installati, gestiti e manutenuti dal Fornitore. Il servizio è realizzato dotando il sistema IPPBX di schede o apparati gateway che interfaccino la rete pubblica (a seconda delle esigenze BRI o PRI ISDN). L'Amministrazione che desidera implementare tale funzionalità deve contrattualizzare l'opzione (per la sede in cui è attivo il servizio CEIP) indicando per ogni sede il numero di canali a 64 Kb/s necessari, secondo un corretto dimensionamento del traffico previsto, per l'interconnessione alla rete pubblica. Il servizio non è comprensivo delle linee di accesso alla RTG e del servizio di gestione del traffico.

[R.187] Il gateway alla base dell'opzione Breakout deve:

- essere dotato di interfacce ISDN BRI o PRI in numero tale da soddisfare i requisiti di traffico espressi dall'Amministrazione;
- includere funzionalità di encoding, echo cancellation, transcodifica.

[R.188] L'opzione Breakout si intende comprensiva di tutte le caratteristiche e funzionalità necessarie al mantenimento del piano di numerazione.

7.1.1.2 Precondizioni e vincoli per la sottoscrizione dei servizi CEIP

[RR.103] I servizi CEIP comprendono la gestione del traffico VOIP nell'ambito Intranet di ciascuna Amministrazione e non sono comprensivi:

- della connettività IP necessaria al trasporto nella CN RUPAR-SPC dei flussi informativi facenti parte del servizio CEIP. Ciascuna Amministrazione deve necessariamente dimensionare opportunamente i propri servizi di trasporto RUPAR-SPC in funzione delle risorse richieste dai servizi VoIP;
- del servizio di gestione del traffico RTG (commutazione del traffico su rete telefonica pubblica e relativo rilegamento trasmissivo);
- della fornitura dei terminali telefonici né di altre tipologie di apparati d'utente, che possono essere acquistati dalle Amministrazioni nell'ambito dei servizi di gestione degli Endpoint successivamente descritto (cfr. § 7.1.4).

7.1.2 Servizi di Gateway (GWTD e GWIP)

I servizi di Gateway si articolano in:

- Servizi di Gateway TDM (GWTD)
- Servizi di Gateway IP (GWIP)

[R.190] Il Punto di accesso al servizio (PAS) per i servizi Gateway è definito come l'insieme delle interfacce verso la LAN dell'Amministrazione sugli apparati che erogano il servizio in sede della Amministrazione.

[RR.104] I servizi di Gateway TDM (GWTD) consistono nella fornitura, messa in opera, gestione e manutenzione di un'infrastruttura di IP Voice Gateway in grado di interconnettere il PABX TDM-based esistente presso una sede dell'Amministrazione con il IP-PBX fornito mediante il servizio CEIP, trasformando il traffico voce in traffico IP; la soluzione prevede pertanto un apparato gateway presso l'Amministrazione connesso al PABX TDM-based di proprietà della stessa, che possa interagire con la sede dove è attivato un servizio CEIP. Si sottolinea che le attività di manutenzione e configurazione del PABX TDM-based esistente presso la sede dell'Amministrazione non sono oggetto di fornitura e sono quindi da ritenersi a completo carico della medesima.

[RR.105] I servizi di Gateway IP (GWIP) consistono nella fornitura, messa in opera, gestione e manutenzione di un'infrastruttura in grado di interfacciare il centralino IP-PBX di proprietà dell'Amministrazione (installata presso locali della stessa) con il IP-PBX (installato presso locali nella sede dell'Amministrazione con profilo CEIP), consentendo in tal modo un collegamento ai servizi VoIP dell'infrastruttura di proprietà dell'Amministrazione. Si sottolinea che le attività di manutenzione e configurazione dell'IP-PBX esistente presso la sede dell'Amministrazione non sono oggetto di fornitura e sono quindi da ritenersi a completo carico della medesima.

[R.193] Deve essere garantita l'interoperabilità tra i differenti servizi di Gateway acquistati da diverse Amministrazioni afferenti al Fornitore.

[R.194] I servizi devono integrarsi completamente rispetto alle infrastrutture preesistenti, con riferimento alle reti locali delle Amministrazioni e al piano di numerazione dei derivati telefonici che, a richiesta dell'Amministrazione, deve poter essere mantenuto. Quindi all'Amministrazione deve essere garantita la possibilità di:

- riutilizzare numerazioni interne già in uso;
- utilizzare nuove estensioni;
- disporre di un piano di numerazione ex-novo utilizzando una diversa radice.

[R.195] Devono essere erogate funzionalità di gestione della segnalazione per il controllo dei vari stati di una chiamata. Tali funzionalità possono in particolare essere declinate in:

- Incoming Call Gateway: funzione deputata alla gestione della segnalazione al fine del corretto instradamento delle chiamate;
- Call Control Function: funzione deputata all'attivazione, rilascio e gestione/cambiamento degli stati della chiamata, nonché alla determinazione della necessità delle operazioni di transcodifica. Gestisce inoltre la registrazione delle differenti postazioni VoIP ed è in grado di interfacciarsi con server esterni dedicati all'implementazione di servizi a valore aggiunto;
- Serving Profile Database: funzione deputata alla gestione e controllo dei profili delle utenze (es. autorizzazione, abilitazioni, ecc.);
- Address Handling: funzione deputata all'analisi, traduzione, eventuale modifica e risoluzione degli indirizzi da identificativo alfanumerico a indirizzo IP.

Il sistema utilizzato deve supportare il protocollo SIP.

[R.196] Ferma restando la responsabilità delle Amministrazioni nella realizzazione, dimensionamento e gestione delle reti LAN interne, la configurazione degli apparati (Gateway) installati per la fornitura del servizio deve essere tale da minimizzare problemi di congestione di traffico della rete locale.

[R.197] I servizi di Gateway devono prevedere funzionalità di trattamento del segnale audio (echo cancellation).

[RR.106] I servizi di Gateway devono garantire funzionalità di autenticazione e autorizzazione nei confronti degli utenti abilitati. Tali funzionalità devono essere implementate per il tramite di comunicazioni logiche IP sicure. A titolo esemplificativo ma non esaustivo, i possibili meccanismi di autenticazione sono: autenticazione basata su MD5 (HTTP Digest) integrata in SIP, Radius, Password dinamiche generate per il tramite di token, One Time Password (OTP), ecc.. Il Fornitore può proporre in alternativa un diverso schema di autenticazione, che deve essere approvato in fase di collaudo del servizio, purché la comunicazione tra la stazione di gestione e l'apparato gestito sia protetta dall'uso di un adeguato algoritmo crittografico.

[R.199] Come detto, per quanto riguarda i servizi di Gateway l'apparato gateway deve essere installato dal Fornitore presso la sede indicata dall'Amministrazione. Per quanto detto, in caso di architetture multisede, il prezzo viene sempre calcolato sulla somma di tutte le utenze afferenti alla totalità delle sedi dell'Amministrazione per le quali è stato attivato il servizio.

[RR.107] I servizi di Gateway sono raggruppati in fasce:

Profilo	Descrizione
GWIP-1	Gateway IP - 30 utenze
GWIP-2	Gateway IP - Da 31 a 100 utenze
GWIP-3	Gateway IP - Da 101 a 300 utenze
GWIP-4	Gateway IP - Oltre 300 utenze
GWTD-1	Gateway TDM - 30 utenze
GWTD-2	Gateway TDM - Da 31 a 100 utenze
GWTD-3	Gateway TDM - Da 101 a 300 utenze
GWTD-4	Gateway TDM - Oltre 300 utenze

[R.200] Il prezzo relativo alla prima fascia dei servizi di Gateway prevede l'acquisto di un numero minimo di 30 utenze.

7.1.2.1 Opzioni dei servizi di Gateway

[R.201] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi di Gateway:

- **Finestra di erogazione estesa** (cfr. [R.6]]).

7.1.2.2 Precondizioni e vincoli per la sottoscrizione dei servizi di Gateway

[R.202] I servizi di Gateway possono essere acquistati esclusivamente in abbinamento ai servizi CEIP.

7.1.3 Servizio di Resilienza Periferica (RESI)

[R.203] I servizi RESI offrono alle Amministrazioni la possibilità di aggiungere caratteristiche di affidabilità ai servizi CEIP che costituiscono la "piattaforma base di servizio" VoIP.

[R.204] I servizi RESI consistono nell'erogazione di un servizio di sopravvivenza locale della sede periferica di un'Amministrazione che ha contrattualizzato il servizio CEIP; RESI viene implementato tramite la fornitura, installazione, gestione e manutenzione di un apparato IP-PBX presso la sede periferica dell'Amministrazione. Tale apparato deve consentire la raccolta delle registrazioni dei terminali IP ivi presenti al fine di garantire il funzionamento locale della sede anche in caso di "mancata connessione" con la sede in cui è attivo CEIP. A seguito di contrattualizzazione del servizio RESI, in caso di mancato collegamento, per qualsiasi causa, con la sede in cui è attivo CEIP, i terminali della sede periferica possono comunicare fra loro e, attraverso l'opzione di breakout, collegarsi eventualmente con la RTG. Più specificatamente, il collegamento con la RTG tramite l'opzione di breakout deve essere disponibile anche quando sia disponibile la connessione con la sede in cui è attivo CEIP. In pratica, il gateway locale di sopravvivenza, in assenza del collegamento con il sistema master della sede principale, assume il ruolo di nuovo apparato master limitatamente a tutti gli apparati della sede periferica coinvolta. Una volta ripristinato il collegamento fra la sede principale e la sede periferica, in automatico deve essere garantito il ripristino delle normali condizioni operative registrando gli apparati della sede periferica sull'apparato master della sede principale. Se l'Amministrazione vuole implementare tale funzionalità su più sedi, deve contrattualizzare il servizio RESI per ciascuna singola sede, acquistandolo per "n" utenti, ove "n" è il numero degli utenti attestati sulla specifica sede.

[R.205] I servizi RESI si intendono comprensivi di tutte le caratteristiche e funzionalità necessarie al mantenimento del piano di numerazione.

7.1.3.1 Opzioni dei servizi RESI

[R.206] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi RESI:

- **Affidabilità elevata** (cfr. [R.207])
- **Finestra di erogazione estesa** (cfr. [R.6])
- **Breakout** (cfr. [R.208], [R.209] e [R.210])

[R.207] L'opzione **Affidabilità elevata** prevede, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto con riferimento al servizio RESI, la duplicazione dell'apparato fornito, gestito e mantenuto dal Fornitore presso la specifica sede dell'Amministrazione. Il secondo apparato è installato nel medesimo locale tecnico ove è installato l'apparato primario. Il servizio prevede la configurazione in hot-standby dei due apparati e quindi la possibilità di mantenimento trasparente della chiamata in corso in caso di guasto.

[R.208] L'opzione **Breakout** prevede, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto per il profilo RESI, l'erogazione di un servizio di interfacciamento con la rete telefonica pubblica (breakout) realizzato tramite schede o apparati gateway forniti, installati, gestiti e manutenuti dal Fornitore. Il servizio incontra le esigenze di quelle Amministrazioni che vogliono garantire affidabilità e continuità di servizio anche in assenza del collegamento dati principale. Il servizio è realizzato dotando il sistema IP-PBX con schede o apparati gateway che interfacciano la rete pubblica (a seconda delle esigenze BRI o PRI ISDN). L'Amministrazione che desidera implementare tale funzionalità deve contrattualizzare l'opzione (per la sede in cui è attivo il servizio RESI) indicando per ogni sede il numero di canali a 64 Kb/s necessari, secondo un corretto dimensionamento del traffico previsto, per l'interconnessione alla rete pubblica. Il servizio non è comprensivo delle linee di accesso alla RTG e del servizio di gestione del traffico.

[R.209] Il gateway alla base dell'opzione Breakout deve:

- essere dotato di interfacce ISDN BRI o PRI in numero tale da soddisfare i requisiti di traffico espressi dall'Amministrazione;
- includere funzionalità di encoding, echo cancellation, transcodifica.

[R.210] L'opzione Breakout si intende comprensiva di tutte le caratteristiche e funzionalità necessarie al mantenimento del piano di numerazione.

7.1.3.2 Precondizioni e vincoli per la sottoscrizione dei servizi RESI

[R.211] I servizi RESI possono essere acquistati esclusivamente in abbinamento ai servizi CEIP.

7.1.4 Servizio di gestione degli Endpoint (ENIP)

Come descritto in precedenza, i servizi CEIP non sono comprensivi della fornitura dei terminali. Il servizio di gestione degli Endpoint descritto nella presente sezione consiste pertanto in un completamento di tali profili CEIP in modo da offrire alle Amministrazioni un servizio VoIP completo.

[R.212] Il servizio di gestione degli Endpoint si intende comprensivo della fornitura del terminale e delle prestazioni di installazione, configurazione, gestione e manutenzione dello stesso. Per il servizio ENIP-1 le attività di installazione e configurazione si limitano alla messa a disposizione del software installabile con relative licenze ed al supporto remoto alla configurazione. Per i Servizi ENIP-2, ENIP-3, ENIP-4, ENIP-5 ed ENIP-9 le attività di installazione si limitano alla consegna degli endpoint presso la sede dell'Amministrazione ed al supporto remoto alla configurazione.

[R.213] Tutti i terminali devono essere compatibili con i servizi VoIP descritti nel presente Capitolato e con le funzionalità/opzioni richieste (cfr. § 5.1.1 e § 5.1.3).

[R.214] Gli apparati previsti dal listino sono:

- ENIP-1: soft-phone
- ENIP-2: telefono IP wired – Entry level model
- ENIP-3: telefono IP wired – Top level model
- ENIP-4: telefono IP wireless
- ENIP-5: postazione audio-conference
- ENIP-6: postazione operatore SW
- ENIP-7: postazione operatore ipovedente
- ENIP-8: postazione operatore non vedente
- ENIP-9: Analog Terminal Adapter (ATA)

[R.215] Il soft-phone (ENIP-1), tramite l'installazione su PC, notebook, ecc. di un client software fornito nell'ambito del servizio, consente all'utente di:

- effettuare/ricevere chiamate telefoniche;

- usufruire di funzionalità di:
  - Presence: indicazione grafica dello stato di presenza (o meno) degli utenti abilitati al servizio ENIP-1;
  - Instant Messaging: funzionalità di invio e ricezione di messaggi testo in tempo reale fra gli utenti abilitati al servizio ENIP-1;
  - File Transfer: scambio file fra utenti abilitati al servizio ENIP-1;
  - Document sharing: condivisione remota di documenti elettronici in tempo reale fra gli utenti abilitati al servizio ENIP-1 che condividono una sessione di lavoro (web collaboration);
  - Videochiamata, fra utenti abilitati al servizio ENIP-1.

[R.216] L'endpoint ENIP-1, nel rispetto delle funzionalità obbligatorie di cui al requisito precedente, deve essere dotato almeno delle seguenti caratteristiche:

- installabile ed eseguibile sui seguenti sistemi operativi: Microsoft Windows XP e successivi, Apple MacOS 10.6 e successive;
- compatibile con lo standard XMPP;
- supporto del protocollo SIP, implementazione della funzione di SIP User Agent e compatibilità con protocolli open di messaggistica istantanea e presenza basati su XML (secondo la XMPP Standard Foundations);
- gestione della buddy list (o lista dei contatti) e funzionalità di tipo click-to-dial;
- supporto di funzionalità di composizione, risposta, trasferta, hold, mute.

[R.217] Il servizio ENIP-1 non è comprensivo della fornitura dei PC o di altro hardware su cui i soft-phone possono essere installati né di eventuali sistemi di interfacciamento con l'utente quali microfono, cuffie o cornette USB.

[R.218] Il telefono IP wired – Entry level model (ENIP-2) deve essere dotato almeno delle seguenti caratteristiche:

- switch interno con porte Ethernet 10/100 e rilevamento automatico della presenza di un PC connesso;
- supporto tele-alimentazione remota attraverso l'interfaccia Ethernet (IEEE 802.3af);
- supporto dello standard IEEE 802.1q;
- kit di alimentazione locale;
- supporto dello standard IETF RFC213 per l'assegnazione dinamica dell'indirizzo IP mediante il protocollo DHCP;
- supporto del protocollo SIP e implementazione della funzione di SIP User Agent;
- schermo monocromatico;
- display a 20 caratteri;
- tastiera alfanumerica;
- regolazione del volume del ricevitore;
- modalità di ascolto viva voce;
- servizio di guida in linea integrato per le operazioni di programmazione.

[R.219] Il telefono IP wired - Top model (ENIP-3) deve essere dotato almeno delle seguenti caratteristiche:

- switch interno con porte Ethernet 10/100 e rilevamento automatico della presenza di un PC connesso;
- supporto tele-alimentazione remota attraverso l'interfaccia Ethernet (IEEE 802.3af);
- supporto dello standard IEEE 802.1q;
- kit di alimentazione locale;

- supporto dello standard IETF RFC213 per l'assegnazione dinamica dell'indirizzo IP mediante il protocollo DHCP;
- supporto del protocollo SIP e implementazione della funzione di SIP User Agent;
- touch screen;
- display a colori 320 x 240 pixel;
- rubrica personale;
- slot per moduli aggiuntivi;
- regolazione del volume del ricevitore;
- modalità di ascolto viva voce;
- 10 tasti hardware o equivalenti software programmabili;
- messaggi di notifica su display multilingua (almeno italiano e inglese);
- servizio di guida in linea integrato per le operazioni di programmazione.

[RR.108] Il telefono IP wireless (ENIP-4) non richiede un collegamento wired alla LAN dell'Amministrazione ma viene connesso a questa in modalità Wi-Fi tramite opportuni access point messi a disposizione dall'Amministrazione; il terminale deve essere dotato almeno delle seguenti caratteristiche:

- assegnazione dinamica dell'indirizzo IP mediante il protocollo DHCP;
- supporto dello standard IEEE 802.11b/g/n;
- supporto del protocollo SIP e implementazione della funzione di SIP User Agent;
- funzionalità WPA e WPA2;
- monitor LCD;
- blocco tasti;
- regolazione del volume del ricevitore;
- 4 tasti programmabili;
- rubrica personale;
- autonomia: almeno 24 ore in stand-by e almeno 4 ore in conversazione;

[R.221] La postazione audio-conference (ENIP-5) consente a più utenti presenti nella stessa stanza (es. sala riunioni) di effettuare/ricevere chiamate telefoniche, con dispositivi privi di cornetta telefonica, in modalità esclusivamente vivavoce. L'apparato deve essere dotato almeno delle seguenti caratteristiche:

- collegamento alla rete IP tramite connessione Ethernet;
- supporto tele-alimentazione remota attraverso l'interfaccia Ethernet (IEEE 802.3af);
- supporto del protocollo SIP e implementazione della funzione di
- SIP User Agent;
- kit di alimentazione locale;
- modalità di ascolto viva voce;
- microfono con copertura a 360°;
- tecnologia full duplex;
- tasto mute.

[R.222] La postazione operatore SW (ENIP-6) consente all'utente tutte le operazioni inerenti la gestione delle chiamate entranti dal proprio PC. La postazione operatore SW è intesa come una applicazione software dotata almeno delle seguenti caratteristiche:

- installabile ed eseguibile almeno sui seguenti sistemi operativi: Microsoft Windows XP e successivi, Apple MacOS 10.6 e successivi;
- tutte le funzioni accessibili tramite l'utilizzo della tastiera del computer e/o del mouse;
- interfaccia grafica user friendly che consenta il rapido accesso a tutte le funzionalità disponibili;

- funzionalità di fonia disponibili analoghe a quelle di un softphone con l'utilizzo di un auricolare/microfono;
- visualizzazione del numero e della tipologia di chiamate in attesa;
- visualizzazione delle informazioni relative al chiamante, delle chiamate in attesa e dello stato di occupato degli utenti di tutta la rete;
- possibilità di risposta, inoltro e gestione (es. messa in attesa, ecc.) delle chiamate entranti.

[R.223] La postazione operatore SW (ENIP-6) costituisce inoltre la componente di base per i servizi ENIP-7 (postazione operatore ipovedente) e ENIP-8 (postazione operatore non vedente), nel senso che i servizi ENIP-7 e ENIP-8 si intendono comprensivi, oltre che delle caratteristiche specifiche descritte nel seguito, di quanto indicato al [R.222]. Quindi tutte le funzionalità di cui al predetto requisito precedente saranno a disposizione degli operatori non vedenti/ipovedenti per il tramite delle componenti speciali di cui ai requisiti specifici che seguono.

[R.224] La postazione operatore ipovedente (ENIP-7) deve essere dotata almeno delle seguenti componenti speciali aggiuntive rispetto alle caratteristiche/funzionalità descritte per la postazione operatore SW (cfr. [R.222]):

- funzionalità di sintetizzatore vocale, con lettura automatica del testo in italiano;
- software di tipo "screen magnifier" per ingrandimento dello schermo.

[R.225] La postazione operatore non vedente (ENIP-10) deve essere dotata almeno delle seguenti componenti speciali aggiuntive rispetto alle caratteristiche/funzionalità descritte per la postazione operatore SW (cfr. [R.222]):

- funzionalità di sintetizzatore vocale, con lettura automatica del testo in italiano;
- barra Braille piezoelettrica da 40 caratteri in grado di rappresentare tutte le combinazioni del codice ASCII.

[R.226] L'Analog Terminal Adapter (ENIP-9) consente l'utilizzo di terminali analogici (es. telefoni analogici, fax, ecc.) nell'ambito di un'infrastruttura Full-IP. L'adattatore deve essere dotato almeno delle seguenti caratteristiche:

- disponibilità di una porta Ethernet di connessione alla rete IP;
- disponibilità di due porte FXS;
- supporto del protocollo SIP;
- supporto del protocollo T.38.

[R.227] Il Punto di accesso al servizio (PAS) per i servizi ENIP è definito come l'interfaccia verso la LAN dell'Amministrazione sugli apparati che erogano il servizio in sede della Amministrazione (si esclude il caso dei soft-phone).

7.1.4.1 Opzioni del servizio ENIP

[R.228] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio ENIP:

- **Finestra di erogazione estesa** (cfr. [R.6]), col vincolo che la finestra di erogazione del servizio ENIP coincida con quella del servizio CEIP associato.

7.1.4.2 Precondizioni e vincoli per la sottoscrizione del servizio Endpoint

[R.229] I servizi di gestione degli Endpoint possono essere acquistati esclusivamente in abbinamento ai servizi CEIP (eventualmente in numero differente rispetto al numero di utenze abilitate ai servizi CEIP).

7.2 Servizi di Telepresenza

I servizi di Telepresenza, comprendono:

- Servizi di Gestione dell'Infrastruttura di Telepresenza (ITEP)
- Servizi di Gestione degli Endpoint di Telepresenza (ETEP)

[R.230] I servizi di Telepresenza si intendono autonomi rispetto ai servizi VoIP nel senso che, fermo il rispetto dei vincoli nel seguito specificati, non è richiesta alcuna integrazione fra le infrastrutture (es. apparati server centrali, ecc.) a supporto delle due tipologie di servizio.

7.2.1 Servizio di gestione dell'Infrastruttura di Telepresenza (ITEP)

I servizi ITEP sono riferiti alla componente centralizzata del servizio e come tali costituiscono il substrato dei servizi di Telepresenza, rappresentando in tal senso la componente obbligatoria e propedeutica per l'eventuale acquisto degli altri servizi (ETEP) presenti nel suddetto listino.

[R.231] I servizi di gestione dell'infrastruttura di telepresenza sono articolati in due distinte modalità di erogazione del servizio (differente profilo di servizio contrattualizzabile dall'Amministrazione):

- **Profilo ITEP-1**: consiste nella fornitura dei servizi di un'infrastruttura di Telepresenza, non necessariamente dedicata alla singola Amministrazione, in modalità Hosted e quindi attraverso sistemi locati presso la Server Farm del Fornitore SPC. Il servizio non prevede ulteriori apparati presso le sedi dell'Amministrazione; i terminali utente possono essere acquistati nell'ambito del servizio aggiuntivo ETEP, descritto successivamente;
- **Profilo ITEP-2**: consiste nella fornitura, messa in opera, gestione in modalità Managed (on-site) e manutenzione di un'infrastruttura di Telepresenza e prevede pertanto l'installazione degli apparati centrali presso una sede dell'Amministrazione; i terminali utente possono essere acquistati nell'ambito del servizio aggiuntivo ETEP, descritto successivamente.

[R.232] I servizi devono essere comprensivi di funzionalità di scheduling che consentano la prenotazione centralizzata delle sessioni di telepresenza. La soluzione deve garantire inoltre funzionalità di convocazione automatica delle sessioni basata su e-mail.

[R.233] Il sistema deve consentire la piena interoperabilità tra postazioni in alta definizione (HD) e postazioni in definizione standard (SD).

[R.234] Deve essere inclusa nel servizio la configurazione dei "canali di videocomunicazione" richiesti dall'Amministrazione, ossia del numero di chiamate audio/video attivabili contemporaneamente da/verso la sede.

[R.235] Il profilo ITEP-1 deve consentire ai partecipanti di collegarsi alle sessioni di telepresenza sia attraverso IP che attraverso connessioni multicanale ISDN. Il profilo ITEP-2 deve consentire ai partecipanti di collegarsi alle sessioni di telepresenza attraverso IP.

[RR.109] Nel caso del profilo ITEP-1 l'infrastruttura Hosted che fornisce il servizio deve essere raggiungibile in IP dalle Amministrazioni mediante la connettività RUPAR-SPC attraverso l'ambito RUPAR. Per permettere la partecipazione di client esterni alla CN RUPAR-SPC il servizio deve essere raggiungibile anche tramite Internet e attraverso linee ISDN RTG. La connettività ISDN dei client del sistema non è inclusa nei servizi ed è fornita a carico dell'Amministrazione. La configurazione del servizio non deve permettere la transizione di traffico diretto tra gli ambiti Internet, Infranet e RUPAR.

[R.237] Il servizio deve garantire la conformità almeno ai seguenti standard:

- H.323 ITU-T Recommendations e SIP (Session Initiation Protocol – RFC 2543) per quanto concerne la segnalazione;
- H.460 ITU-T Recommendations per quanto concerne la funzionalità di NAT e Firewall traversal;

- RTP (Real time Transport Protocol - RFC 3550) per quanto riguarda la trasmissione in tempo reale dei dati su rete IP;
- H.264 ITU-T Recommendations per quanto concerne la codifica video;
- G.711 e AAC-LD (Advanced Audio Coding with Low Delay) per quanto riguarda la codifica audio.

[R.238] Il servizio deve consentire funzionalità di trasferimento di file e di visualizzazione, condivisione e revisione di documenti fra i vari partecipanti alla sessione.

[R.239] La soluzione deve consentire funzionalità di invito e partecipazione degli utenti ad una sessione nonché funzionalità di moderazione della stessa.

[R.240] I servizi devono prevedere funzionalità di trattamento del segnale audio (echo cancellation).

[R.241] La soluzione deve consentire la memorizzazione, per almeno 6 mesi solari, delle informazioni elencate:

- utenti coinvolti e rispettive Amministrazioni di appartenenza,
- data e ora di inizio della sessione,
- data e ora di fine della sessione.

[RR.110] Il servizio si intende comprensivo della disponibilità di una interfaccia verso servizi di "directory centralizzata" secondo lo standard LDAP v3 al fine di memorizzare e consultare una rubrica indirizzi.

[R.243] Il sistema messo a disposizione dell'Amministrazione per il servizio di profilo ITEP 2 deve avere le seguenti caratteristiche minime:

- Interfaccia LAN 100 Mb/s Ethernet o superiore
- Capacità di gestire contemporaneamente almeno 10 continuous presence ports a 1080p x 30 (risoluzione x fotogrammi al secondo)

7.2.1.1 Opzioni del servizio ITEP

[RR.111] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per i servizi ITEP:

- **Affidabilità elevata** (cfr. [R.245]), applicabile esclusivamente al profilo di servizio ITEP-2;
- **Registrazione delle sessioni** (cfr. [R.246]), applicabile ad entrambi i profili ITEP-1 e ITEP-2;
- **Finestra di erogazione estesa** (cfr. [R.6]), applicabile esclusivamente al profilo di servizio ITEP-2.

[R.245] L'opzione di **Affidabilità elevata** prevede, per il profilo di servizio ITEP-2, la completa ridondanza dell'infrastruttura di servizio.

[R.246] L'opzione di **Registrazione delle sessioni** prevede, per entrambi i profili ITEP-1 e ITEP-2:

- la memorizzazione di sessioni di video conferenza a cui si può accedere successivamente per rivedere la sessione registrata;
- la disponibilità delle seguenti informazioni:
  - utenti coinvolti e rispettive Amministrazioni di appartenenza;
  - data e ora di inizio della sessione;
  - data e ora di fine della sessione.

7.2.1.2 Precondizioni e vincoli per la sottoscrizione del servizio ITEP

[R.247] I servizi ITEP non sono comprensivi della connettività IP necessaria al trasporto su SPC dei flussi informativi facenti parte del servizio ITEP. Ciascuna Amministrazione deve

necessariamente dimensionare opportunamente i propri servizi di trasporto SPC in funzione delle risorse richieste dai servizi ITEP.

7.2.2 Servizio di gestione degli ENDPOINT di telepresenza (ETEP)

[R.248] Come descritto in precedenza, i servizi ITEP non sono comprensivi della fornitura degli Endpoint. Il servizio ETEP consiste pertanto nella fornitura, installazione, configurazione e gestione di una serie di Endpoint, a completamento del servizio di Telepresenza, che prevedano modalità di connessione IP (non è richiesta connettività ISDN). Per i servizi ETEP-1 ed ETEP-2 le attività di installazione e configurazione si limitano alla messa a disposizione del software installabile con relative licenze ed al supporto remoto alla configurazione. Per i Servizi ETEP-3 le attività di installazione si limitano alla consegna degli endpoint presso la sede dell'Amministrazione ed al supporto remoto alla configurazione.

[R.249] Tutti i terminali devono essere compatibili con i servizi ITEP descritti e con le funzionalità richieste nel [R.231].

[R.250] Gli apparati previsti dal listino sono:

- ETEP-1: client SW per PC;
- ETEP-2: client SW per dispositivi mobili;
- ETEP-3: postazione da tavolo;
- ETEP-4: postazione base;
- ETEP-5: postazione evoluta.

[R.251] Gli apparati previsti per i profili ETEP-3, ETEP-4 e ETEP-5 devono essere dotati di interfaccia Fast Ethernet o superiore.

[R.252] Il client SW per PC (ETEP-1) deve essere dotato almeno delle seguenti caratteristiche:

- fruizione del servizio a seguito di installazione su PC, notebook, ecc. di un client software fornito nell'ambito del servizio;
- installabile ed eseguibile almeno sui seguenti sistemi operativi: Microsoft Windows XP e successivi, Apple MacOS 10.6 e successivi.

[R.253] Il servizio ETEP-1 non è comprensivo della fornitura del PC o di altro hardware su cui i client SW possono essere installati né di eventuali sistemi di interfacciamento con l'utente quali microfono, cuffie, ecc.

[R.254] Il client SW per dispositivi mobili (ETEP-2) deve essere dotato almeno delle seguenti caratteristiche:

- fruizione del servizio a seguito di installazione su smartphone o tablet;
- installabile ed eseguibile almeno sui seguenti sistemi operativi per dispositivi mobili: Apple iOS 6 o successive release, Android 4.0 o successive release, Microsoft Windows 8 o successive release.

[RR.111] La postazione da tavolo (ETEP-3) identifica un sistema di videoconferenza ad alta qualità per una postazione e deve essere dotata almeno delle seguenti caratteristiche:

- n° 1 schermo LCD, LED o al Plasma ad almeno 32", con qualità video High Definition – 720p;
- n° 1 telecamera con risoluzione HD;
- sistema audio con qualità CD full-duplex;
- microfono direzionale (eventualmente integrato nella telecamera);
- telecomando;
- interfaccia utente con funzioni di Rubrica e menù multilingua.

[RR.112] La postazione base (ETEP-4) deve essere dotata almeno delle seguenti caratteristiche:

- n° 1 schermo LCD, LED o al Plasma ad almeno 60", con qualità video High Definition – 720p;
- base di appoggio a terra o a parete;
- n° 1 telecamera con risoluzione HD;
- sistema audio con qualità CD full-duplex;
- strumenti di controllo audio (cancellatori di eco, riduzione automatica del rumore);
- microfono direzionale (eventualmente integrato nella telecamera);
- telecomando;
- interfaccia utente con funzioni di Rubrica e Menù multilingua.

[RR.113] La postazione evoluta (ETEP-5) deve essere dotata almeno delle seguenti caratteristiche:

- n° 2 schermi LCD, LED o al Plasma ad almeno 42", con qualità video High Definition – 720p;
- base di appoggio a terra o a parete;
- n° 1 telecamera con risoluzione HD;
- sistema audio con qualità CD full-duplex;
- strumenti di controllo audio (cancellatori di eco, riduzione automatica del rumore);
- microfono direzionale (eventualmente integrato nella telecamera);
- telecomando;
- interfaccia utente con funzioni di Rubrica e Menù multilingua.

7.2.2.1 Opzioni del servizio ETEP

[R.258] Di seguito sono elencate le opzioni sottoscrivibili, a fronte della corresponsione di un canone aggiuntivo rispetto a quanto previsto dal servizio base, per il servizio ETEP:

- **Finestra di erogazione estesa** (cfr. [R.6])

7.2.2.2 Precondizioni e vincoli per la sottoscrizione del servizio ETEP

[R.259] I servizi ETEP possono essere acquistati esclusivamente in abbinamento ai servizi ITEP (eventualmente in numero differente rispetto al numero di utenze abilitate ai servizi ITEP).

8 SERVIZI DI SUPPORTO PROFESSIONALE (SSUP)

I Servizi di Supporto Professionale (SSUP) consistono in attività professionali erogate dal Fornitore alle Amministrazioni ad integrazione dei servizi già descritti nel presente Capitolato.

I Servizi di Supporto Professionale sono caratterizzati da un insieme di attività opzionali ad elevato valore aggiunto per l'identificazione di scenari di ottimizzazione dell'efficienza, della qualità intrinseca e percepita del servizio stesso, dell'utilizzo e di massimizzazione del valore per l'Amministrazione.

[RR.114] I Servizi di Supporto Professionale sono facoltativi.

[RR.115] I servizi di supporto non includono attività riconducibili al ciclo di vita del servizio acquistato dall'Amministrazione nell'ambito della CN RUPAR-SPC, il quale comprende:

- Definizione del servizio;
- Analisi dei requisiti;
- Progettazione della soluzione;
- Realizzazione della soluzione progettata;
- Collaudo;
- Documentazione relativa al servizio erogato;

- Messa in esercizio;
- Manutenzione, gestione e assistenza.

[R.261] Tutte queste attività sono da considerarsi incluse nella fornitura del servizio acquistato dall'Amministrazione, e non rientrano nel perimetro dei servizi di supporto.

[R.262] Viene definito un ciclo di vita per i servizi di supporto, complementare al ciclo di vita del servizio acquistato dall'Amministrazione (cfr.[RR.115]). Il ciclo di vita per i servizi di supporto prevede tre fasi distinte:

- **Supporto alla definizione della strategia di servizio**: include attività utili a raccogliere informazioni sugli asset dell'Amministrazione, a valutare la fattibilità dell'introduzione di un servizio e a valutare i vantaggi ottenibili attraverso l'introduzione del servizio stesso;
- **Supporto all'introduzione del servizio**: include attività che consentono all'Amministrazione di pianificare l'introduzione del servizio e di introdurlo in maniera efficiente ed efficace;
- **Supporto all'operatività del servizio**: include attività che supportano l'Amministrazione nell'utilizzo ottimale del servizio e nell'acquisizione di eventuali certificazioni di conformità a standard e normative.

[R.263] Nell'ambito delle fasi "Supporto all'introduzione del servizio" e "Supporto all'operatività del servizio", possono essere erogati servizi di formazione del personale dell'Amministrazione.

[R.264] I servizi di supporto oggetto del presente Capitolato comprendono:

- Servizi di Supporto specialistico (SSUP)
- Servizi di Formazione (FORM)

[R.265] I servizi di supporto professionale non prevedono alcun PAS.

8.1 Servizi di Supporto Specialistico (SSUS)

I Servizi di Supporto Specialistico (SSUS) sono articolati in:

- Supporto al servizio di trasporto (STRA)
- Supporto al servizio di sicurezza (SSIC)
- Supporto al servizio di comunicazione evoluta (SSCE)

[R.266] Il servizio di supporto specialistico è erogato secondo il modello "accordo quadro a consumo". Il costo della prestazione professionale è quantificato in termini di giorni/uomo, differenziato in base al profilo professionale del professionista impiegato.

[R.267] Per tutti i SSUP sono previsti tre diversi profili professionali che possono essere impiegati per l'erogazione dei servizi di supporto specialistico:

- Team Leader;
- Specialista Senior;
- Specialista.

[R.268] Il ruolo principale del Team Leader consiste nel pianificare le attività da svolgere e coordinare lo svolgimento del progetto.

[R.269] Il ruolo principale dello Specialista Senior consiste nel fornire supporto specialistico durante l'esecuzione delle attività di progetto e nel coordinare e contribuire alla redazione della documentazione di progetto. Lo Specialista Senior è responsabile delle attività che gli vengono affidate.

[R.270] Il ruolo principale dello Specialista consiste nel fornire supporto specialistico e contribuire alla redazione della documentazione di progetto.

[R.271] Per ognuno dei singoli servizi di supporto, sono definiti più profili, come di seguito elencato:

- Supporto al servizio di trasporto (STRA-1);
- Supporto alla definizione di reti IPv6 (STRA-2);
- Supporto di base alla sicurezza (SSIC-1);
- Sistema di gestione della sicurezza delle informazioni (SSIC-2);
- Incident Management (SSIC-3);
- Business Continuity (SSIC-4);
- Supporto al servizio di comunicazione evoluta (SSCE-1);

[R.272] Ogni attività di supporto acquistata dall'Amministrazione, sia essa di supporto specialistico o di formazione, deve essere riconducibile ad una delle tipologie di servizio elencate in [R.271] e ad una delle fasi elencate in [R.262]. Di conseguenza, ogni attività di supporto, sia essa di supporto specialistico o di formazione, deve essere definita e documentata esplicitando:

- La tipologia di servizio di riferimento (cfr. [R.271]);
- La fase del ciclo di vita all'interno della quale l'attività si configura (cfr. [R.262]).

[R.273] A seconda della tipologia di servizio di supporto specialistico erogata, sono previsti differenti requisiti minimi inderogabili che caratterizzano i profili professionali di Team Leader, Specialista Senior e Specialista. Questi requisiti sono descritti in dettaglio nelle successive sezioni dedicate alle diverse tipologie di servizio di supporto specialistico.

[R.274] Per ognuna delle tre fasi definite in [R.262], sono definite le tipologie dei prodotti dell'attività di supporto specialistico e lo skill mix minimo che fissa delle percentuali minime di utilizzo delle diverse figure professionali definite in [R.267], come illustrato nella seguente tabella:

Fase	Prodotti della fase	Percentuali minime di utilizzo delle figure professionali
Supporto alla definizione della strategia di servizio	• Assessment degli asset dell'Amministrazione • Studio di fattibilità dell'introduzione di un servizio.	Team Leader: 10% Specialista Senior: 20% Specialista: 40%.
Supporto all'introduzione del servizio	• Piano di migrazione; • Pianificazione dell'introduzione del servizio.	Team Leader: 10% Specialista Senior: 20% Specialista: 40%.
Supporto all'operatività del servizio	• Report dell'attività svolta; • Documentazione specifica relativa al servizio erogato	Team Leader: 10% Specialista Senior: 20% Specialista: 50%.

[R.275] Lo skill mix definito per ogni fase (cfr. [R.274]), deve essere applicato solo in caso di servizi di supporto di durata maggiore o uguale a 10 giornate uomo di lavoro. In caso di attività che richiedono un effort inferiore, non è previsto nessuno skill mix minimo.

8.1.1 Servizi di supporto al trasporto (STRA)

[R.276] Per il servizio di supporto al trasporto, le figure professionali da fornire devono essere caratterizzate dai requisiti minimi inderogabili riportati nella seguente tabella:

Profilo	Titolo di studio	Esperienze lavorative	Conoscenze
Team Leader	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 12 anni di cui almeno 6 nella specifica funzione. • Significative esperienze di direzione di progetti complessi nell'area delle telecomunicazioni in contesti multidisciplinari e multi servizi. • Stima di tempi e risorse necessari per la realizzazione di un progetto. • Responsabilità di gruppi di progetto.	• Certificazione ITILv3 Foundation. • Certificazione di Project Management (ad esempio PMIPMP, Prince2 Practitioner, Senior Project manager Level BIPMA). • Modelli di acquisto e gestione di servizi tecnologici nel settore Pubblico. • Tecniche e metodi di project management. • Tecniche e metodi di quality management, norme ISO, modalità di certificazione. • Tecnologie e soluzioni per servizi di connettività (wired e wireless). • Progettazione e realizzazione di reti di telecomunicazioni. • Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese.
Specialista Senior	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 8 anni di cui almeno 5 nella specifica funzione. • Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni, in contesti multidisciplinari e multi servizi. • Esperienza nell'utilizzo di metodologie di project management. • Capacità di problem solving.	• Certificazione ITILv3 Foundation. • Se esistente, certificazione rilasciata dal vendor dei prodotti utilizzati dal Fornitore per l'erogazione del servizio di trasporto. • Mercato e tendenze evolutive delle telecomunicazioni. • Tecnologie e soluzioni per servizi di connettività (wired e wireless). • Progettazione e realizzazione di reti di telecomunicazioni. • Procedure di monitoraggio e auditing di progetti. • Buona conoscenza della lingua inglese.
Specialista	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 4 anni di cui almeno 2 nella specifica funzione. • Partecipazione a gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni	• Architetture di soluzioni di telecomunicazioni. • Reti di telecomunicazioni basati su protocolli standard.

[R.277] In aggiunta alle certificazioni previste per ogni profilo professionale ed elencate in [R.276], sono richieste ulteriori caratteristiche che dipendono dalla specifica tipologia di servizio di trasporto e dal profilo professionale considerato, come dettagliato nella seguente tabella:

Profilo servizio	Profilo professionale	Caratteristiche aggiuntive richieste
STRA-1	Team Leader	• N/A
	Specialista Senior	• Modelli di definizione e monitoraggio di Service Level Agreement.
	Specialista	• Principali metodiche di rilevazione dei livelli di servizio
STRA-2	Team Leader	• N/A
	Specialista Senior	• Conoscenza dei protocolli IPv6, piani di indirizzamento IPv6, tecniche di integrazione IPv4-IPv6, multicasting IPv6
	Specialista	• Conoscenza dei protocolli IPv6, tecniche di integrazione IPv4-IPv6

8.1.1.1 Precondizioni e vincoli per la sottoscrizione del servizio STRA

[R.278] Le Amministrazioni possono acquistare il servizio di supporto al trasporto se e solo se hanno acquistato almeno un servizio di trasporto.

[R.279] Se un'Amministrazione decide di avvalersi del servizio di supporto al trasporto, la spesa minima per tale attività è fissata pari a 2.000,00 Euro.

[R.280] La spesa massima per attività di supporto al trasporto (inclusi relativi servizi di formazione correlati), fermo restando il vincolo sulla spesa minima di cui al [R.279], è fissata:

- per i servizi STRA-1, al 5% della spesa totale sostenuta dall'Amministrazione per i servizi di trasporto,
- per i servizi STRA-2, al 10% della spesa totale sostenuta dall'Amministrazione per i servizi di trasporto.

8.1.2 Servizi di supporto alla sicurezza (SSIC)

[R.281] Il servizio di supporto alla sicurezza comprende quattro diversi profili di servizio di supporto:

- Supporto di base alla sicurezza (SSIC-1);
- Sistema di gestione della sicurezza delle informazioni (SSIC-2);
- Incident Management (SSIC-3);
- Business Continuity (SSIC-4).

[R.282] Per tutti i profili del servizio SSIC le figure professionali utilizzate devono essere caratterizzate dai seguenti requisiti minimi inderogabili:

Profilo	Titolo di studio	Esperienze lavorative	Conoscenze
Team Leader	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione). .	• Esperienza complessiva non inferiore a 12 anni di cui almeno 6 nella specifica funzione. • Significative esperienze di direzione di progetti complessi nell'area della sicurezza in contesti multidisciplinari e multi servizi. • Stima di tempi e risorse necessari per la realizzazione di un progetto. • Responsabilità di gruppi di progetto.	• Certificazione ITILv3 Foundation. • Certificazione di Project Management (ad esempio PMIPMP, Prince2 Practitioner, Senior Project manager Level BIPMA). • Modelli di acquisto e gestione di servizi tecnologici nel settore Pubblico. • Tecniche e metodi di project management. • Tecniche e metodi di quality management, norme ISO, modalità di certificazione. • Tecnologie e soluzioni per servizi di sicurezza. • Progettazione e realizzazione di soluzioni di sicurezza. • Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese.
Specialista Senior	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 8 anni di cui almeno 5 nella specifica funzione. • Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle sicurezza, in contesti multidisciplinari e multi servizi. • Esperienza nell'utilizzo di metodologie di project management. • Capacità di problem solving.	• Certificazione ITILv3 Foundation. • Se esistente, certificazione rilasciata dal vendor dei prodotti utilizzati dal Fornitore per l'erogazione del servizio di trasporto. • Mercato e tendenze evolutive della sicurezza. • Tecnologie e soluzioni per servizi di sicurezza. • Progettazione e realizzazione di soluzioni di sicurezza. • Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese
Specialista	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 4 anni di cui almeno 2 nella specifica funzione. • Partecipazione a gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni e della sicurezza	• Architetture di soluzioni di telecomunicazioni. • Reti di telecomunicazion i basati su protocolli standard. • Soluzioni di sicurezza. • Principali metodiche di rilevazione dei livelli di servizio

[R.283] In aggiunta alle certificazioni previste per ogni profilo professionale ed elencate in [R.282], sono richieste ulteriori certificazioni che dipendono dalla specifica tipologia di servizio di sicurezza e dal profilo professionale considerato, come dettagliato nella seguente tabella:

Profilo servizio	Profilo professionale	Caratteristiche aggiuntive richieste
SSIC-1	Team Leader	• N/A
	Specialista Senior	• Certificazione di Project Management (ad esempio PMI-PMP, Prince2 Practitioner, Senior Project manager Level B-IPMA). • Certificazione di sicurezza (ad esempio ISACA CISA, ISACA CISM, (ISC)2 CISSP, (ISC)2 SSCP).
	Specialista	• N/A
SSIC -2	Team Leader	• Certificazione ISO/IEC 27001 Lead Auditor.
	Specialista Senior	• Certificazione ISO/IEC 27001 Lead Auditor.
	Specialista	• N/A
SSIC-3	Team Leader	• Certificazione ISO/IEC 20001:2005.
	Specialista Senior	• Certificazione ITILv3 Service Operation. • Certificazione ISO/IEC 20001:2005.
	Specialista	• N/A
SSIC -4	Team Leader	• Certificazione ISO/IEC 20001:2005.
	Specialista Senior	• Certificazione ITILv3 Service Operation. • Certificazione ISO/IEC 20001:2005.
	Specialista	• N/A

8.1.2.1 Precondizioni e vincoli per la sottoscrizione del servizio SSIC

[R.284] Le Amministrazioni possono acquistare il servizio di supporto alla sicurezza se e solo se hanno acquistato almeno un servizio di sicurezza.

[R.285] Se un'Amministrazione decide di avvalersi del servizio di supporto alla sicurezza, la spesa minima per tale attività è fissata pari a 5.000,00 Euro.

[R.286] La spesa massima per attività di supporto alla sicurezza (inclusi relativi servizi di formazione correlati) è fissata pari al 20% della spesa totale sostenuta dall'Amministrazione per i servizi di sicurezza, fermo restando il vincolo minimo definito in [R.285].

8.1.3 Servizi di supporto alla Comunicazione evoluta (SSCE)

[R.287] Per il servizio di supporto alla comunicazione evoluta, le figure professionali da fornire devono essere caratterizzate dai requisiti minimi inderogabili riportati nella seguente tabella:

Profilo	Titolo di studio	Esperienze lavorative	Conoscenze
Team Leader	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione). .	• Esperienza complessiva non inferiore a 12 anni di cui almeno 6 nella specifica funzione. • Significative esperienze di direzione di progetti complessi nell'area delle telecomunicazioni in contesti multidisciplinari e multi servizi. • Stima di tempi e risorse necessari per la realizzazione di un progetto. • Responsabilità di gruppi di progetto.	• Certificazione ITILv3 Foundation. • Certificazione di Project Management (ad esempio PMIPMP, Prince2 Practitioner, Senior Project manager Level BIPMA). • Modelli di acquisto e gestione di servizi tecnologici nel settore Pubblico. • Tecniche e metodi di project management. • Tecniche e metodi di quality management, norme ISO, modalità di certificazione. • Tecnologie e soluzioni per servizi di comunicazione evoluta (VoIP, Unified Communication e Telepresenza). • Progettazione e realizzazione di reti di telecomunicazioni. • Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese.
Specialista Senior	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 8 anni di cui almeno 5 nella specifica funzione. • Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni, in contesti multidisciplinari e multi servizi. • Esperienza nell'utilizzo di metodologie di project management. • Capacità di problem solving.	• Certificazione ITILv3 Foundation. • Se esistente, certificazione rilasciata dal vendor dei prodotti utilizzati dal Fornitore per l'erogazione del servizio di trasporto. • Mercato e tendenze evolutive delle telecomunicazioni. • Tecnologie e soluzioni per servizi di comunicazione evoluta (VoIP, Unified Communication e Telepresenza). • Progettazione e realizzazione di reti di telecomunicazioni. • Procedure di monitoraggio e auditing di progetti. • Modelli di definizione e monitoraggio di Service Level Agreement. • Buona conoscenza della lingua inglese.
Specialista	Laurea o cultura equivalente (la cultura equivalente, per non laureati, corrisponde a 4 anni di anzianità in più sia per l'esperienza complessiva che per la specifica funzione).	• Esperienza complessiva non inferiore a 4 anni di cui almeno 2 nella specifica funzione. • Partecipazione a gruppi di lavoro nell'ambito di progetti di realizzazione nell'area delle telecomunicazioni	• Architetture di soluzioni di telecomunicazioni. • Reti di telecomunicazioni basati su protocolli standard. • Architetture e standard relativi alle comunicazioni multimediali. • Principali metodiche di rilevazione dei livelli di servizio

8.1.3.1 Precondizioni e vincoli per la sottoscrizione del servizio SSCE

[R.288] Le Amministrazioni possono acquistare il servizio di supporto alla comunicazione evoluta se e solo se hanno acquistato almeno un servizio di comunicazione evoluta.

[R.289] Se un'Amministrazione decide di avvalersi del servizio di supporto alla comunicazione evoluta, la spesa minima per tale attività è fissata pari a 2.000,00 Euro.

[R.290] La spesa massima per attività di supporto alla comunicazione evoluta (inclusi relativi servizi di formazione correlati) è fissata pari al 5% della spesa totale sostenuta dall'Amministrazione per i servizi di comunicazione evoluta, fermo restando il vincolo minimo definito in [R.289].

8.2 Servizi di Formazione (FORM)

[R.291] I Servizi di Formazione (FORM), si articolano in:

- Servizi di formazione in aula (FONS)
- Servizi di formazione remota (FREM)

[R.292] I servizi di formazione sono sottoposti a valutazione svolta attraverso un questionario i cui contenuti e modalità di somministrazione verranno concordati tra il fornitore assegnatario e l'amministrazione e che prevede sei livelli di valutazione: ottimo, buono, discreto, sufficiente, scarso, insufficiente.

[R.293] Il costo della formazione è quantificato in termini di costo di un giorno di formazione.

8.2.1 Servizi di Formazione in aula (FONS)

[R.294] I servizi di formazione in aula consistono nell'erogazione di un servizio di formazione da parte di un docente in presenza degli alunni.

[R.295] Il servizio di formazione in aula comprende una giornata di lezione (pari a 8 ore di lezione). In caso di necessità, l'Amministrazione può acquistare un numero maggiore di giornate di formazione in aula.

[R.296] Il servizio di formazione in aula comprende la preparazione del materiale didattico, consistente in un documento (di testo o presentazione con slide), che sarà rilasciato agli alunni iscritti al corso.

[R.297] Il servizio di formazione in aula è disponibile in tre diverse modalità di erogazione (differenti profili di servizio contrattualizzabili dall'Amministrazione):

- **Profilo FONS-1**: consiste nell'erogazione di 8 ore di formazione per un numero di alunni minore o pari a 30. L'aula dove si svolge l'attività di formazione è messa a disposizione dall'Amministrazione che acquista il servizio di formazione, e deve essere dotata almeno di un video proiettore. L'aula dove si svolge la formazione si può trovare in qualsiasi comune sul territorio regionale pugliese.
- **Profilo FONS-2**: consiste nell'erogazione di 8 ore di formazione per un numero di alunni minore o pari a 30. L'aula dove si svolge l'attività di formazione è messa a disposizione dal Fornitore, e deve essere dotata almeno di un video proiettore e, su richiesta dell'Amministrazione, di una lavagna. L'aula dove si svolge la formazione deve essere situata in una città capoluogo di provincia della Regione Puglia scelta dall'Amministrazione che acquista il servizio di formazione.
- **Profilo FONS**-3: questo profilo ha le stesse caratteristiche del profilo FONS-2. La differenza consiste nel fatto che, in questo caso, l'aula messa a disposizione dal Fornitore deve essere dotata, oltre che di un video proiettore anche di una postazione pc con connessione a Internet per ogni alunno.

[R.298] Il servizio di formazione in aula deve essere erogato da un docente che abbia almeno 5 anni di esperienza nell'attività formativa relativamente alla specifica tipologia di servizio di supporto trattata. In alternativa, il docente deve aver progettato/gestito almeno 3 interventi formativi nella tematica nei tre anni precedenti alla contrattualizzazione del servizio.

8.2.1.1 Precondizioni e vincoli per la sottoscrizione del servizio FONS

[R.299] Al momento dell'acquisto del servizio di formazione in aula, l'Amministrazione deve specificare a quale tipologia di servizio di supporto tale attività si riferisce (cfr. [R.271]).

[R.300] Le Amministrazioni possono acquistare il servizio di formazione in aula, relativamente ad una specifica tipologia di supporto, se e solo se hanno acquistato almeno un servizio rispetto al quale la formazione fa riferimento.

[R.301] Il costo del servizio di formazione in aula contribuisce al calcolo per la spesa totale massima sostenibile per i servizi di supporto, definita per ogni singola tipologia di servizio di supporto.

8.2.2 Servizi di Formazione remota (FREM)

[R.302] I servizi di formazione remota consistono nell'erogazione di un servizio di formazione attraverso una piattaforma accessibile dagli alunni via web. L'accesso a Internet e la postazione pc attraverso cui l'alunno accede al servizio di formazione remota non sono inclusi nel servizio.

[R.303] Il servizio di formazione remota comprende una giornata di lezione (pari a 8 ore). In caso di necessità, l'Amministrazione può acquistare un numero maggiore di giornate di formazione remota.

[R.304] Il servizio di formazione remota comprende la gestione della piattaforma accessibile via web e la preparazione del materiale didattico, consistente in un documento (di testo o presentazione con slide), che sarà rilasciato agli alunni iscritti al corso.

[R.305] Il servizio di formazione remota è disponibile in due diverse modalità di erogazione (differenti profili di servizio contrattualizzabili dall'Amministrazione):

- **Profilo FREM-1**: (formazione in telepresenza) consiste nell'erogazione di un servizio di formazione attraverso una piattaforma accessibile via web, per un numero di alunni minore pari a 100. Questo profilo di servizio prevede l'erogazione di 8 ore di lezione in formato video in diretta. Un docente illustra la lezione e gli alunni, in real-time, seguono la lezione (audio e video) tramite una postazione pc. Il servizio comprende quindi la gestione della piattaforma, la docenza per 8 ore di lezione, la realizzazione del materiale didattico e un servizio di tutoraggio attraverso cui gli alunni possono richiedere informazioni o spiegazioni al docente via email per un periodo pari a sette giorni solari dall'erogazione del corso.
- **Profilo FREM-2**: (formazione in differita) consiste nell'erogazione di un servizio di formazione attraverso una piattaforma accessibile via web, per un numero di alunni minore pari a 100. Questo profilo di servizio prevede l'erogazione di materiale didattico in formato di documento di testo o presentazione con slide per un self training stimato di 8 ore. Il servizio comprende quindi la gestione della piattaforma, la realizzazione del materiale didattico e un servizio di tutoraggio attraverso cui gli alunni possono richiedere informazioni o spiegazioni al docente via email per un periodo pari a trenta giorni solari dal giorno in cui il materiale didattico è stato reso disponibile agli alunni.

[R.306] La docenza inclusa nel servizio di formazione remota FREM-1 e FREM-2 deve essere erogata da un docente che abbia almeno 5 anni di esperienza nell'attività formativa relativamente alla specifica tipologia di servizio di supporto trattata. In alternativa, il docente deve aver progettato/gestito almeno 3 interventi formativi nella tematica nei tre anni precedenti alla contrattualizzazione del servizio.

8.2.2.1 Precondizioni e vincoli per la sottoscrizione del servizio FREM

[R.307] Al momento dell'acquisto del servizio di formazione remota, l'Amministrazione deve specificare a quale tipologia di servizio di supporto tale attività si riferisce (cfr. [R.271]).

[R.308] Le Amministrazioni possono acquistare il servizio di formazione remota, relativamente ad una specifica tipologia di supporto, se e solo se hanno acquistato almeno un servizio rispetto al quale la formazione fa riferimento.

[R.309] Il costo del servizio di formazione remota contribuisce al calcolo per la spesa totale massima sostenibile per i servizi di supporto, definita per ogni singola tipologia di servizio di supporto.

9 SERVIZI DI GESTIONE E MANUTENZIONE

I Servizi di Gestione e Manutenzione riguardano le seguenti attività:

- Provisioning, Configuration e Change Management
- Supervisione della rete e analisi delle prestazioni dei servizi
- Fault Management
- Rendicontazione

[R.310] Il Fornitore del servizio è responsabile della gestione e della manutenzione di tutte le componenti del servizio erogato fino alla frontiera di responsabilità definita dal punto di accesso al servizio (PAS).

[RR.116] Il Fornitore, come parte integrante del servizio, nell'ambito della attività di Provisioning, Configuration e Change Management, deve provvedere:

- all'attivazione e alla cessazione di nuovi servizi e delle relative componenti;
- all'installazione e alla configurazione degli apparati: il Fornitore deve garantire l'effettiva installazione degli apparati per la fornitura dei servizi acquistati dall'Amministrazione. Il Fornitore deve consegnare all'Amministrazione un inventario degli apparati installati. L'Amministrazione è responsabile di mettere a disposizione del Fornitore adeguati spazi e sottoservizi (es. alimentazione elettrica, condizionamento, ecc.) secondo quanto indicato dal Fornitore nelle attività di Site Preparation (cfr.§ 11);
- all'installazione del software: il Fornitore deve farsi carico delle attività di installazione del software sugli apparati, compreso il caricamento e l'attivazione di nuove release software su tutti i sistemi utilizzati e l'aggiornamento software degli apparati per l'allineamento con i rilasci software messi a disposizione dai fornitori della tecnologia, sia con finalità di patching che relativamente all'introduzione dei nuovi servizi;
- all'attuazione degli adeguamenti, riconfigurazioni o ristrutturazioni richiesti da attività di "system tuning";
- al trasloco interno, inteso come lo spostamento, all'interno della medesima sede dell'Amministrazione, nel caso in cui le esigenze operative dell'Amministrazione stessa lo richiedano, delle componenti tecnologiche utilizzate per l'erogazione del servizio, fermo restando la responsabilità dell'Amministrazione di mettere a disposizione del fornitore ambienti ed infrastrutture di supporto adeguate a quanto previsto nelle specifiche riguardanti la predisposizione dei siti ("Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi" allegato all'originale Progetto dei Fabbisogni).

[R.312] La realizzazione delle attività di Trasloco di un servizio tra due sedi dell'Amministrazione (Trasloco Esterno), saranno realizzate e contabilizzate in maniera analoga ad una attivazione del servizio presso la nuova sede (in particolare quindi con la corresponsione di una nuova Una Tantum, se prevista) e una disattivazione presso la vecchia sede, fermo restando l'obbligo del Fornitore a garantire la piena operatività dell'Amministrazione in tutte le fasi del Trasloco, ad esempio:

- Permettendo la sostituibilità dei due servizi (ad esempio garantendo il riutilizzo degli Indirizzi IP statici della sede cessante nella nuova sede).
- Mantenendo attivo il servizio cessante fino alla completa attivazione del servizio nella nuova sede.
- Garantendo con adeguate procedure la possibilità di eseguire un Roll back dei servizi se si verificassero problemi nella transizione tra le due sedi.

[R.313] Le attività di gestione e manutenzione devono essere erogate all'interno della finestra temporale contrattualizzata dall'Amministrazione, a scelta tra quella standard (definita nel requisito [R.5]) o quella estesa (definita nel requisito [R.6]).

[R.314] Fermo restando la necessità di ridurre al minimo le interruzioni o ostacoli all'operatività dell'Amministrazione, il Fornitore può concordare con l'Amministrazione intervalli di

"Manutenzione Programmata" preventiva, (ad es. al fine di realizzare necessarie attività di test, aggiornamenti di release software, ecc.). Nell'intervallo concordato per tali attività, eventuali malfunzionamenti del servizio non incideranno sul calcolo di SLA e Penali, purché il servizio sia completamente e correttamente ripristinato al termine dell'intervallo programmato.

[RR.117] Per l'espletamento delle attività di Fault Management, Supervisione e gestione delle risorse utilizzate per l'erogazione dei servizi e analisi delle prestazioni dei servizi, il Fornitore deve dotarsi di un Centro di Gestione di rete di seguito indicato come Network Operating Center (**NOC**) e di un Centro di Gestione per la sicurezza di seguito indicato come Security Operating Center (**SOC**), non necessariamente dedicati ai servizi della CN RUPAR-SPC, integrato con le strutture di supporto utenti del proprio Help Desk, in modo da assicurare, nel complesso, i livelli di servizio contrattualizzati.

[RR.118] Il NOC del Fornitore, limitatamente alla propria infrastruttura di rete, deve disporre di un sistema, non necessariamente dedicato ai servizi della CN RUPAR-SPC, basato su architetture e tecnologie standard di tipo SNMP, rivolto alla gestione delle risorse utilizzate per erogare i servizi SPC. Attraverso tale sistema il Fornitore deve verificare in modo continuativo le prestazioni della propria infrastruttura di rete al fine di:

- gestire la rete, con monitoraggio puntuale di ogni servizio;
- valutare il grado di occupazione delle risorse trasmissive;
- verificare il corretto dimensionamento complessivo del sistema;
- consentire una verifica dei livelli di servizio contrattualmente stabiliti ed il calcolo di statistiche.

[RR.119] Il SOC del Fornitore ha il compito di gestire le risorse utilizzate per erogare i servizi di sicurezza e deve svolgere anche i compiti di Unità Locale di Sicurezza SPC previsti dalle Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività[1].

[RR.120] Il Fornitore deve nominare all'interno del SOC un Responsabile Operativo della sicurezza che dovrà fungere da punto di contatto prioritario per tutte le problematiche di sicurezza che interessano i servizi di sicurezza della CN RUPAR-SPC.

[RR.121] Il SOC del Fornitore, centralizzando e monitorando tutte le attività di security (analisi del rischio, vulnerability assessment, generazione di reportistica ed informative, etc.) attraverso un approccio di tipo logico-procedurale (asset analysis, risk management, security policy ecc.), deve verificare in modo continuativo le prestazioni della propria infrastruttura al fine di:

- gestire i sistemi utilizzati per l'erogazione dei servizi di sicurezza, con monitoraggio puntuale di ogni servizio per la gestione preventiva dei rischi;
- verificare il corretto dimensionamento complessivo dei sistemi;
- consentire una verifica dei livelli di servizio contrattualmente stabiliti ed il calcolo di statistiche.

[R.316] Il Fornitore deve rendere disponibile alle Amministrazioni un help desk di 2° livello, che riceva segnalazioni di malfunzionamento esclusivamente dai centri di gestione di 1° livello della singola Amministrazione; tale help desk deve essere raggiungibile, per la ricezione di segnalazioni ed apertura di ticket, almeno nei seguenti modi:

- via pagina web, con accesso 24X7 365 giorni l'anno;
- via fax, con accesso 24X7 365 giorni l'anno;
- via call center contattabile attraverso Numero Verde, disponibile per ciascuna Amministrazione nell'orario della finestra per cui è stato contrattualizzato il servizio (finestra standard o estesa).

[1] Cfr. Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 - Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale».

[RR.122] Il Fornitore deve dotarsi di uno strumento di Trouble Ticketing per consentire la gestione ed il monitoraggio delle attività di fault management.

[RR.123] Anche il CTRP deve poter aprire dei Trouble Ticket (TT) verso il FSR, a seguito di incongruenze nate dall'osservazione dei dati raccolti in maniera autonoma. E' compito del FSR mettere a disposizione del CTRP gli strumenti necessari per aprire i TT presso i propri sistemi.

[RR.124] L'apertura di un TT da parte di una Amministrazione, afferente ad un determinato FSR, può generare i seguenti casi:

- il problema segnalato è interno al fornitore che deve risolverlo;
- il problema è interno alla CN RUPAR-SPC e quindi il fornitore deve inoltrare il TT al CTRP, che riconcilia eventuali TT aperti da altri fornitori relativamente allo stesso problema e lo risolve;
- il problema è interno ad un altro fornitore della CN RUPAR-SPC e quindi il CTRP inoltra il TT a quel fornitore, che deve risolverlo;
- il problema è interno alla QXN (Qualified eXchange Network) e quindi il CTRP inoltra il TT al proprio provider del servizio di interconnessione alla QXN che deve risolverlo.

[RR.125] In particolare, all'interno del SOC o tra il SOC e i punti esterni, il FSR deve garantire i seguenti flussi di informazione:

- flusso tra il SOC del FSR ed il responsabile operativo del SOC di un altro fornitore della CN RUPAR-SPC o più in generale del SPC: rappresenta sia la segnalazione, in caso di escalation, di problemi sul servizio erogato in modalità cooperativa e su cui il fornitore ha la competenza, sia le richieste/risposte di attivazione/(ri)configurazione/sospensione di servizi che richiedono l'intervento congiunto dei SOC di più fornitori;
- flusso tra il SOC del FSR ed il SOC del CTRP: realizza lo scambio informativo relativo a:
  - la ricezione dal SOC del CTRP delle procedure operative e del materiale informativo per l'implementazione delle direttive emesse a garanzia del livello minimo di sicurezza della CN RUPAR-SPC;
  - le informazioni fornite al SOC del CTRP dal FSR durante una sessione di audit volta a verificare che il fornitore rispetti il livello minimo di sicurezza imposto sulla CN RUPAR-SPC;
  - lo scambio di informazioni (log, istruzioni di test e verifiche, contromisure, etc.) con il SOC del CTRP per la gestione, degli incidenti informatici che coinvolgono il fornitore nell'ambito dei servizi erogati sulla CN RUPAR-SPC o più in generale sul SPC e che impattano sul livello minimo di sicurezza imposto sulla stessa;
  - lo scambio di informazioni con il SOC del CTRP, che avrà anche funzione di CERT-R, per intraprendere le azioni necessarie all'analisi e alla gestione degli incidenti informatici e degli abusi che impattano sul livello minimo di sicurezza imposto nella CN RUPAR-SPC e sul SPC
- flusso tra il SOC del FSR e il referente della CN RUPAR-SPC dell'Amministrazione; realizza lo scambio informativo relativo a:
  - la ricezione dall'Amministrazione delle procedure operative e del materiale informativo per l'implementazione delle direttive emesse a garanzia del livello di sicurezza del Sistema Informativo dell'Amministrazione;
  - lo scambio di informazioni (log, istruzioni di test e verifiche, contromisure, etc.) per la gestione degli incidenti informatici che coinvolgono il FSR nell'ambito dei servizi erogati sulla CN RUPAR-SPC e che impattano sul livello minimo di sicurezza imposto sulla stessa, o sul livello di sicurezza maggiore assicurato sul dominio dell'Amministrazione.

[RR.126] L'help desk deve dare riscontro alla presa in carico della segnalazione di un disservizio con l'apertura di un trouble ticket, fornendo all'Amministrazione interessata o al CTRP il numero del ticket aperto e una prima diagnosi.

[RR.127] Il Fornitore deve interfacciarsi costantemente con l'Amministrazione interessata o con il CTRP durante le fasi di lavorazione di un trouble ticket, aggiornando l'Amministrazione

sull'avanzamento dei lavori necessari alla risoluzione del disservizio segnalato, concordando preventivamente eventuali interventi presso le sedi dell'Amministrazione, e formalizzando tempestivamente la proposta di chiusura del ticket.

[RR.128] Il Fornitore deve impegnarsi all'apertura proattiva di TT anche in mancanza di segnalazioni da parte dell'Amministrazione, in risposta a malfunzionamenti rilevati dai propri sistemi di gestione.

[RR.129] Il Fornitore deve dotarsi di un sistema che permetta l'erogazione dei seguenti servizi di fatturazione:

- gestione e controllo della fatturazione;
- fornitura dei dati di fatturazione e rendicontazione in formato elettronico (almeno .xls e .csv);
- ripartizione della fatturazione per centro di costo.

[RR.130] In caso di specifiche esigenze da parte dell'Amministrazione o del CTRP in merito al formato dati, il Fornitore deve garantire la propria disponibilità a personalizzare la struttura della documentazione.

[RR.131] Il Fornitore deve garantire alle singole Amministrazioni e al CTRP la disponibilità dei dati, sia analitici che sintetici, su supporto elettronico (almeno .xls e .csv).

[RR.132] Il Fornitore deve rendere disponibili i dati sopra descritti con frequenza bimestrale.

[RR.133] La fatturazione deve essere accompagnata da un report contenente informazioni relative all'erogazione di ogni singolo servizio, nel rispetto delle modalità e dei contenuti degli SLA contrattualizzati. Il sistema di fatturazione del Fornitore deve altresì fornire tutte le informazioni di dettaglio in merito alle sessioni tariffate, nel rispetto sulle norme della privacy in vigore.

[RR.134] A supporto dei Servizi di Gestione e Manutenzione il Fornitore deve realizzare un **Sito Web** per rendere accessibili, da parte del CTRP e dell'Amministrazione (per la parte di propria competenza), le informazioni relative a:

- servizi utilizzati e dettagli amministrativi e tecnici sui servizi; a titolo esemplificativo e non esaustivo devono essere rese disponibili le informazioni relative al Contratto Esecutivo (data di sottoscrizione, data di scadenza, referente dell' Amministrazione e del Fornitore, importo economico totale, data di attivazione dei servizi, elenco dei servizi contrattualizzati dalla Amministrazione e, per ciascun servizio, caratteristiche tecniche, parametri dimensionali, configurazioni e prezzo), indirizzi IP assegnati all'Amministrazione, nonché le copie in formato elettronico del Contratto Esecutivo, del Piano dei Fabbisogni e del Progetto dei Fabbisogni; queste informazioni devono essere sempre mantenute allineate con la situazione esistente rendendo comunque disponibili i dati storici;
- misurazioni dei livelli di servizio che includano almeno i dati oggetto di tutti i report periodici previsti (rif. Allegato 1.1 - Livelli di servizio e penali);
- trouble ticket gestiti dall'help desk;
- dati di riscontro relativi ai SLA;
- dati di fatturazione e di rendicontazione; tali dati essere aggiornati almeno mensilmente ed essere relativi ad almeno gli ultimi sei bimestri.

Deve essere possibile generare report, grafici, e query complesse e devono essere disponibili funzionalità di esportazione dei dati, secondo formati standard.

[RR.135] Il Fornitore, per l'accesso al Sito Web deve fornire credenziali di accesso (username e password) al CTRP e alle Amministrazioni.

10 SERVIZI DI INTERAZIONE CON LE INFRASTRUTTURE CONDIVISE

[RR.136] Il Fornitore è obbligato alla sottoscrizione dei servizi appartenenti alle seguenti categorie:

- Servizi di Interconnessione all'EPO;
- Servizi di Interconnessione QXN;
- Servizi di Governance.

10.1 Servizio di interconnessione all'EPO

Il Servizio di interconnessione all'EPO garantisce la comunicazione via RUPAR alle Amministrazioni aderenti alla CN RUPAR-SPC. L'EPO è ubicato presso il Parco Scientifico Tecnopolis, SP per Casamassima Km.3 70010 Valenzano (BA) ed è completamente ridondato. L'EPO è costituito da due armadi per apparati di comunicazione posizionati in due distinti edifici (edificio A e edifico H), contenenti ciascuno uno switch L3 ad alte prestazioni. L'accesso all'armadio dell'EPO e la gestione dello switch sono di competenza del CTRP che supervisionerà anche il funzionamento dell'intero EPO controllando l'interscambio di informazioni tra le reti dei FSR.

[RR.137] Il Fornitore è obbligato a collegarsi all'EPO in modo ridondato. Per interconnettersi agli switch di EPO il Fornitore deve installare a suo carico all'interno degli armadi di EPO una coppia di Border Router collegati al suo backbone attraverso percorsi fisici e centrali di attestazione distinti.

[RR.138] Ogni Fornitore ha diritto ad allocare in ognuno dei due armadi dell'EPO un solo router dotato di almeno di una scheda Fast-Ethernet/Gigabit-Ethernet per il collegamento allo switch e di una scheda per connessione a linea geografica per il collegamento al resto della rete del Fornitore e, per suo tramite, alle Amministrazioni sue clienti. La scelta del collegamento al EPO in Gigabit Ethernet o in Fast Ethernet è lasciata al FSR che la farà in dipendenza del volume complessivo del traffico scambiato nell'EPO e del rispetto dei requisiti sulla Banda Garantita.

[RR.139] Il Fornitore, per l'housing dei propri router nell'EPO, non sosterrà costi.

[RR.140] I router di un FSR che svolgono servizio per la CN RUPAR-SPC devono essere riservati alla Community Network e non potranno essere utilizzati per servire altri utenti. La riservatezza potrà essere realizzata anche mediante router virtuali che gestiscano VPN dedicate alla CN RUPAR-SPC (VRF).

[RR.141] I router della CN RUPAR-SPC dovranno essere sincronizzati al Tempo Ufficiale di Rete propagato dal CTRP sulla CN RUPAR-SPC o tramite la sincronizzazione con il tempo di riferimento nazionale dell'Istituto Elettrotecnico Nazionale "Galileo Ferraris".

[RR.142] I router dei FSR devono consentire l'accesso in sola lettura via protocollo SNMP da parte del sistema centrale di controllo del CTRP, il cui indirizzo verrà comunicato al FSR al momento dell'abilitazione ad operare: il sistema centrale di controllo del CTRP farà uso, oltre che del protocollo SNMP, anche del protocollo ICMP.

[RR.143] Il traffico Intranet tra sedi di una stessa Amministrazione o il traffico RUPAR di Amministrazioni distinte, collegate alla rete dello stesso FSR, deve svolgersi interamente nel backbone del FSR.

[RR.144] Il traffico tra un'Amministrazione e un soggetto non pubblico, esterno a SPC, deve attraversare il backbone del FSR fino ai NAP pubblici della rete Internet.

[RR.145] Il traffico tra PAL della CN RUPAR-SPC deve transitare esclusivamente o attraverso il backbone del comune fornitore o attraverso il dominio di interconnessione della CN RUPAR-SPC nel caso di PAL servite da fornitori diversi.

[RR.146] Tra due estremi dei flussi di traffico precedentemente descritti, si dovrà sempre avere un routing simmetrico.

[RR.147] Le principali regole di routing che assicurano che i differenti flussi di traffico seguano i percorsi indicati nei requisiti dal [RR.143] al [RR.146] sono:

- ogni FSR deve realizzare nell'EPO sessioni di peering BGP privato con il CTRP; su queste sessioni gli FSR annunceranno esclusivamente le reti riservate alla CN RUPAR-SPC corrispondenti ad Enti da essi gestiti, che verranno definite come appartenenti ad Autonomous System privati (AS numeri da 64512 a 65535, cfr. RFC1930);
- gli stessi FSR dovranno annunciare le reti riservate alla CN RUPAR-SPC di propria pertinenza sull'Internet nazionale ed internazionale mediante la propria connessione ad Internet ed i propri Autonomous System ufficiali all'interno delle loro major network;
- le reti della CN RUPAR-SPC apprese da un FSR nell'EPO, non possono quindi essere propagate nella propria infrastruttura al di là della parte che compete la CN RUPAR-SPC.

10.2 Servizio di interconnessione alla QXN

Il Servizio di interconnessione alla QXN garantisce la comunicazione via Infranet alle Amministrazioni aderenti alla CN RUPAR-SPC. La CN RUPAR-SPC assicura la propria connessione al SPC attraverso le modalità previste dall'Art. 17 comma 5 del DPCM 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del SPC". Nei locali che ospitano l'EPO si realizza anche, per i fornitori regionali, il peering pubblico con l'AS del CTRP funzionale al transito verso la QXN.

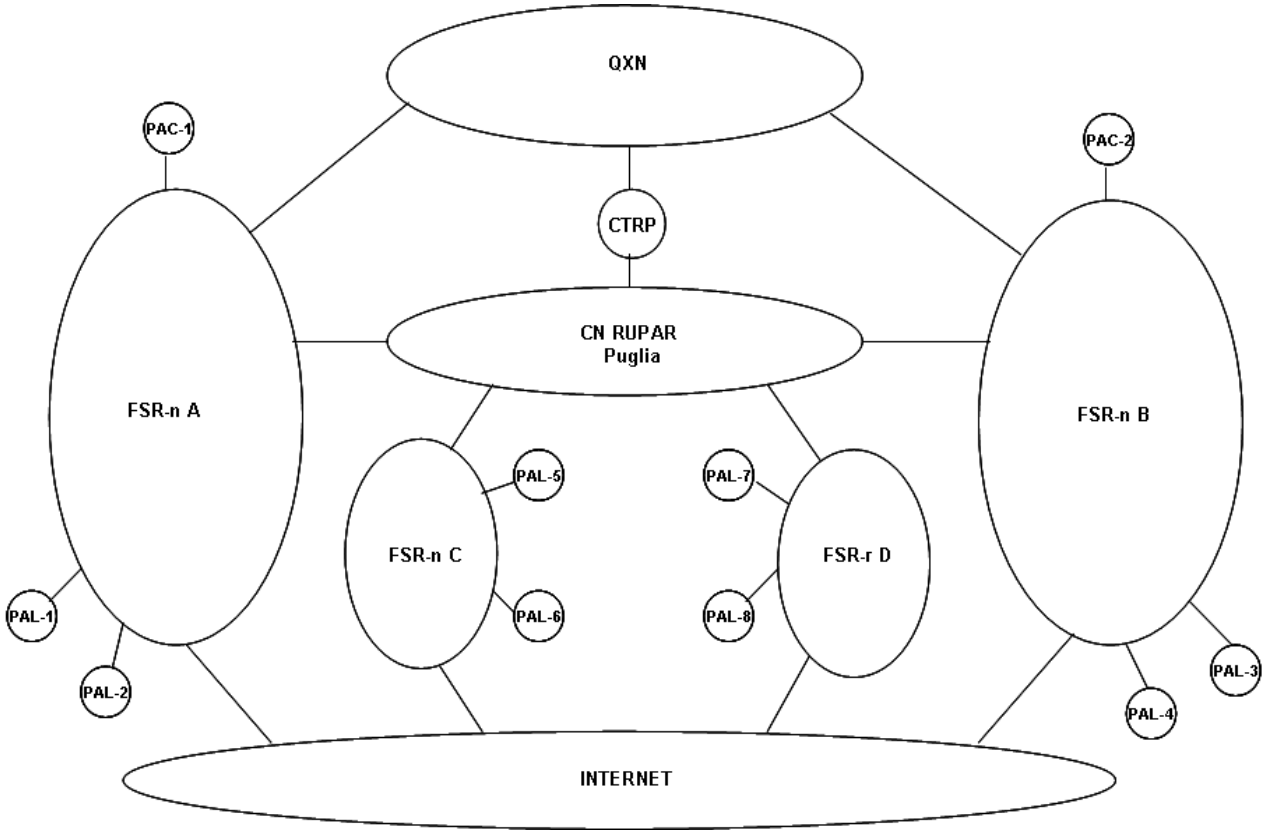
[RR.148] Il traffico tra PAC e PAL servite da FSR regionali dovrà attraversare la QXN e il dominio di interconnessione della CN RUPAR-SPC.

[RR.149] E' ammesso che il traffico tra PAC e PAL servite da FSR nazionali che non vogliono configurarsi come FSR regionali possa transitare direttamente attraverso il backbone del FSR e la QXN senza transitare attraverso il dominio di interconnessione della CN RUPAR-SPC.

[RR.150] Tra due estremi dei flussi di traffico precedentemente descritti, si dovrà sempre avere un routing simmetrico.

[RR.151] Il CTRP è dotato di un AS pubblico per l'interconnessione alla QXN:

- i fornitori regionali che non disporranno di una propria connessione alla QXN possono annunciare alla QXN le reti riservate alla CN RUPAR-SPC attraverso l'Autonomous System (AS) del CTRP che funge da transito verso la QXN; per questo i fornitori regionali dovranno predisporre un peering BGP pubblico specifico con l'AS del CTRP;
- i fornitori nazionali potranno scegliere se configurarsi come un FSR regionale (assumendo un AS pubblico dedicato per la CN RUPAR-SPC) ovvero possono annunciare le reti riservate alla CN RUPAR-SPC direttamente alla QXN mediante le proprie connessioni e con i loro Autonomous System pubblici;
- a titolo di esempio, la successiva figura mostra lo schema di interconnessione tra due ipotetici fornitori nazionali (FSR-n A e FSR-n B), un fornitore nazionale configurato come regionale (FSR-n C), un fornitore regionale (FSR-r D), la CN RUPAR-SPC e la QXN



[RR.152] Il Fornitore è obbligato ad installare a suo carico una coppia di Border Router dotati di almeno di una scheda Fast-Ethernet (uno nell'edificio A e uno nell'edificio H) da interconnettere ai router del CTRP che garantiscono il transito verso la QXN.

10.3 Servizi di Governance

Il CTRP svolge le attività tecniche necessarie per la progettazione, il coordinamento, l'operatività ed il controllo della CN RUPAR-SPC ed è responsabile della qualità delle soluzioni tecniche adottate e dei servizi erogati. Tra le attività del CTRP rientrano:

- il disegno iniziale della CN RUPAR-SPC e delle sue successive evoluzioni;
- la definizione e la diffusione alle Amministrazioni locali ed ai fornitori di servizi, di procedure, schemi e direttive tecniche necessarie per garantire l'unitarietà e la omogeneità della Community Network, elevate prestazioni e sicurezza;
- l'assistenza tecnica alle Amministrazioni Locali per la progettazione e la realizzazione delle parti di loro competenza e per lo sviluppo di nuovi servizi telematici che richiedono il concorso di più enti;
- l'infrastrutturazione e la gestione degli apparati e dei servizi generali necessari per il funzionamento dei nodi di interconnessione tra le reti dei fornitori;
- il controllo sulla qualità dei servizi erogati dai fornitori della CN RUPAR-SPC;
- la supervisione della gestione della sicurezza della CN RUPAR-SPC;
- il coordinamento dei fornitori per la risoluzione di problemi e la realizzazione di miglioramenti;
- attività tecniche di coordinamento a livello Sistema Pubblico di Connettività.

Il CTRP gestisce anche il portale www.rupar.puglia.it che contiene informazioni di carattere generale sulla CN RUPAR-SPC (contesto normativo e tecnico, documentazione tecnico-operativa e contrattuale, ecc.).

[RR.153] Per garantire la corretta governance dei Servizi della CN RUPAR-SPC alle Amministrazioni aderenti, il Fornitore deve ottemperare alle direttive tecniche emanate dal CTRP.

[RR.154] Il Fornitore deve comunicare al CTRP, all'indirizzo cer_ct@pec.rupar.puglia.it, l'avvenuta firma di un nuovo Contratto Esecutivo o la variazione di un Piano dei Fabbisogni entro 10 (dieci) giorni lavorativi dalla data di sottoscrizione dello stesso. Le informazioni di dettaglio e la copia elettronica del Contratto devono essere disponibili sul Sito Web del Fornitore di cui al requisito [RR.134].

[RR.155] Il Fornitore deve comunicare al CTRP, all'indirizzo cer_ct@pec.rupar.puglia.it, l'avvenuta attivazione / disattivazione di un nuovo servizio entro 10 (dieci) giorni lavorativi dalla data di sottoscrizione dello stesso (la comunicazione può comprendere l'indicazione di più attivazioni). Le informazioni di dettaglio devono essere disponibili sul Sito Web del Fornitore di cui al requisito [RR.134].

[RR.156] Il Fornitore deve garantire al CTRP l'accesso in lettura alla Management Information Base (MIB) delle Terminazioni di Rete (TDR) delle Amministrazioni. Le modalità di accesso alle MIB verranno definite dal CTRP in modo tale da garantire la non interferenza con le prestazioni contrattualizzate per il servizio di Trasporto Dati.

[RR.157] Il Fornitore, se richiesto dal CTRP, dovrà interfacciare i propri sistemi informativi con quelli del CTRP per fornire, almeno giornalmente, gli stessi dati contenuti nel Sito Web del Fornitore di cui al requisito [RR.134]. Il FSR dovrà quindi garantire la piena disponibilità ad uniformarsi a modalità di trasmissione dati definite dal CTRP.

[RR.158] Il Fornitore, al fine di consentire al CTRP la segnalazione di disservizi e/o malfunzionamenti e di condurre attività di escalation in caso di problemi tra Amministrazione e Fornitore o tra Fornitori, deve indicare come punto di contatto un referente tecnico responsabile del dialogo diretto col CTRP e un indirizzo di posta elettronica certificata.

11 MODALITA' DI ATTIVAZIONE DEI SERVIZI

Il processo di richiesta ed attivazione dei servizi della CN RUPAR-SPC per la singola Amministrazione si articola nelle seguenti fasi:

- fase contrattuale (comprensiva della fase di rilevazione e progettazione)
- fase di attivazione (comprensiva delle fasi di *site preparation*, installazione ed eventuale migrazione)

Ciascuna Amministrazione dovrà selezionare il fornitore rilanciando il confronto competitivo tra i fornitori che avranno sottoscritto con InnovaPuglia S.p.A. il Contratto Quadro per la fornitura dei Servizi di connettività per la CN RUPAR-SPC. L'Amministrazione dovrà allegare alla richiesta di offerta un documento intitolato "**Piano dei fabbisogni**", contenente le indicazioni sul tipo, le quantità ed il dimensionamento dei servizi richiesti, conforme al modello predisposto dal CTRP che sarà reso disponibile nel portale www.rupar.puglia.it.

[RR.159] Il Fornitore deve effettuare tutte le attività descritte nei requisiti successivi sia nel caso di migrazione di un'Amministrazione da servizi preesistenti sia nel caso di realizzazioni ex novo.

[R.368] Nel caso in cui l'Amministrazione fruisca di servizi preesistenti, il Fornitore deve esplicitamente prevedere, congiuntamente con l'Amministrazione contraente, le procedure di attivazione che permettano il mantenimento dell'operatività durante le fasi di migrazione.

[RR.160] In risposta alla richiesta d'offerta, entro il tempo massimo in essa fissato, i FSR dovranno presentare all'Amministrazione un documento intitolato "**Progetto dei fabbisogni**", nel quale raccoglieranno le richieste dell'Amministrazione contenute nel "Piano dei Fabbisogni" e formuleranno una proposta tecnico/economica.

[RR.161] Il "Progetto dei fabbisogni" dovrà almeno contenere:

- il "*Progetto di Attuazione*": con il dettaglio, per ciascun servizio, di:
  - identificativo del servizio;
  - configurazione;

  - quantità (ove applicabile)
  - data prevista di attivazione.
- il "*Piano di Attuazione*" con:
  - il "*Piano operativo*";
  - il "*Documento programmatico di gestione della sicurezza dell'Amministrazione*";
  - le "*Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi*";
- l'indicazione delle "*Modalità di presentazione e approvazione degli Stati di Avanzamento Mensili*", qualora la tempistica del Piano di attuazione lo richieda.

[R.373] Il Fornitore ha facoltà di condurre, con proprio personale tecnico o altro personale da lui stesso incaricato, e congiuntamente con i referenti dell'Amministrazione interessata, sopralluoghi sui siti, allo scopo di verificare gli impatti e le modalità dell'attivazione dei servizi nella sede in esame (secondo quanto richiesto dall'Amministrazione nel Piano dei fabbisogni).

[R.374] Il Fornitore deve approntare il calendario dei sopralluoghi necessari. Tale calendario deve indicare, per ciascuna sede oggetto di sopralluogo, il nominativo dell'incaricato dal Prestatore per il sopralluogo, con gli estremi di un documento di riconoscimento e l'elenco delle verifiche da effettuare. Il calendario viene sottoposto all'approvazione dell'Amministrazione interessata.

[R.381] Il "Piano di Attuazione" deve includere la descrizione dettagliata delle attività e procedure che il Prestatore metterà in atto nel processo di migrazione dei servizi, al fine di minimizzare l'impatto sull'operatività dei servizi erogati.

[R.383] Il Fornitore deve inoltre fornire un servizio di "project management" che consiste nella pianificazione, gestione e verifica delle attività mirate al completamento del progetto. La definizione delle attività è responsabilità di un gruppo di lavoro costituito almeno da:

- un responsabile del progetto presso la singola Amministrazione;
- un project manager del Fornitore.

[RR.162] A valle della sottoscrizione del Contratto Esecutivo il FSR deve consegnare all'Amministrazione le "*Specifiche di dettaglio delle prove di collaudo"* relative a tutte le tipologie di servizio richieste.

[RR.163] Il Fornitore deve definire, all'interno del Progetto dei Fabbisogni (in particolare all'interno dell'allegato "Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi"), le specifiche riguardanti la predisposizione dei siti.

[R.386] Salvo ove specificamente definito, i servizi non comprendono attività di realizzazione e gestione delle infrastrutture di rete di proprietà dell'Amministrazione (cablaggio strutturato), LAN, fonia TDM e alimentazione presso i siti dell'Amministrazione.

[R.387] Su richiesta dell'Amministrazione, il Fornitore deve provvedere all'esecuzione di attività di posa in opera (cablaggi, apparati di condizionamento, ecc.) che si rendano necessarie per improcrastinabili esigenze realizzative, con un limite di spesa massimo di 5.000 € per sito, così come specificato all'interno del Contratto Quadro.

[R.388] Il Fornitore deve definire, congiuntamente con l'Amministrazione contraente, il piano di installazione dei servizi che deve rispettare i seguenti requisiti minimi:

- gli interventi devono essere effettuati in intervalli orari definiti dall'Amministrazione coerentemente con le proprie esigenze di operatività;
- l'operatività del servizio deve essere garantita anche durante la fase intermedia di test e collaudo;
- l'impatto delle operazioni di roll-out e installazione sulla normale operatività delle sedi deve essere minimo.

[R.389] Qualora un'operazione di installazione dovesse costituire causa di disservizio, il Fornitore deve adoperarsi per garantire un ripristino immediato della condizione preesistente.

[R.390] A partire dalla data di decorrenza del contratto esecutivo, il Fornitore deve procedere all'installazione nelle sedi secondo le modalità temporali previste dal Progetto di Attuazione (cfr. [RR.161]). In fase di configurazione degli apparati di accesso per ogni sede individuata il Fornitore, congiuntamente con l'Amministrazione, deve:

- contattare il referente tecnico della sede;
- concordare le modalità ed i tempi di interventi on-site;
- effettuare una verifica del sito, se necessario;
- procedere all'attestazione del collegamento;
- partecipare alle attività di test ed emettere un verbale per collaudo eseguito con esito positivo.

[R.391] Il Fornitore deve considerare prioritaria, sia nella pianificazione che nell'esecuzione dell'attivazione, la salvaguardia dell'operatività delle Amministrazioni nel periodo di tempo durante il quale avviene la migrazione dei servizi.

[R.392] In particolare, nel caso in cui un'operazione di attivazione del servizio dovesse costituire causa di malfunzionamento, il Fornitore deve assicurare la possibilità di un ripristino immediato della condizione preesistente (procedura di roll-back).

[R.393] Tutti gli interventi eseguiti sulle piattaforme in esercizio devono essere effettuati al di fuori dell'orario di lavoro del personale delle Amministrazioni e, comunque, in intervalli orari definiti dall'Amministrazione coerentemente con le proprie esigenze di operatività.

[R.394] Pur nel rispetto della continuità del servizio, il piano di migrazione proposto dal Fornitore deve consentire il massimo parallelismo delle attività al fine di minimizzare i tempi di attivazione.

Dalla data iniziale di validità del Contratto Quadro, il CTRP garantirà l'interconnessione sull'EPO di Bari dei servizi di trasporto ed interoperabilità degli attuali fornitori con i nuovi, per consentire una transizione senza problemi dalla vecchia infrastruttura alla nuova.

12 COLLAUDI

Nel presente capitolo sono descritte tutte le procedure di collaudo tecnico che il Fornitore deve attuare ai fini della verifica della completa funzionalità dei servizi erogati.

12.1 Prescrizioni Generali

[RR.164] La fornitura dei servizi descritti nel presente capitolato tecnico deve essere soggetta alle seguenti procedure di collaudo tecnico:

- **Collaudo funzionale**: prevede delle prove mirate a verificare le modalità con le quali il Fornitore erogherà i servizi oggetto della presente gara ed è svolto sotto la direzione di una Commissione di collaudo incaricata dalla Stazione Appaltante in contraddittorio col Fornitore.
- **Collaudo di configurazione**: è svolto dalla singola Amministrazione interessata; ogni contratto esecutivo stipulato tra il Fornitore e l'Amministrazione prevede delle prove mirate a verificare la corretta erogazione dei servizi acquisiti dall'Amministrazione.

12.2 Collaudo Funzionale

[RR.165] Il collaudo funzionale dei servizi oggetto della presente gara può essere effettuato secondo modalità e fasi temporali differenti:

- il rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione dei Servizi di Gestione e Manutenzione e dei Servizi di Interazione con le Infrastrutture Condivise deve essere inviato formalmente alla Stazione Appaltante entro novanta (90) giorni solari dalla data di sottoscrizione del Contratto Quadro;

- per i restanti servizi il collaudo funzionale può essere svolto o su piattaforma di *test bed* presso un sito individuato dal Fornitore congiuntamente con la Stazione Appaltante, o contestualmente al Collaudo di Configurazione per la prima Amministrazione che avrà sottoscritto un Contratto Esecutivo con quel tipo di servizio; questo collaudo tecnico avrà anche valore di Certificazione del Servizio nel senso che le Amministrazioni che replicheranno il Servizio potranno decidere se ridurre le proprie attività di collaudo tecnico.

[RR.166] Per ogni servizio le verifiche verranno svolte secondo le specifiche proposte dal Fornitore attraverso un documento intitolato "*Specifiche di dettaglio delle prove di collaudo del servizio …*", allegato con la Documentazione di Riscontro (cfr. 13.1) al rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione del servizio inviato alla Stazione Appaltante e da questi approvato. Questo documento dovrà contenere almeno:

- la descrizione dell'ambiente di test;
- l'elenco delle prove di collaudo;
- sistema di misura dei livelli di servizio e di generazione della reportistica;
- modalità di svolgimento delle prove di collaudo.

[RR.167] La Commissione di Collaudo sarà comunque libera di indicare criteri e modalità proprie di collaudo che, a suo insindacabile giudizio, rispondano in modo più compiuto all'esigenza di verificare i servizi.

[RR.168] Il Fornitore deve anche fornire a proprie spese e con espressa impossibilità di rivalersi sulla Stazione Appaltante, mezzi, personale ed ogni altra strumentazione necessari all'esecuzione delle prove.

12.3 Collaudo di Configurazione

[RR.169] In seguito alla stipula del Contratto Esecutivo con la singola Amministrazione, il Fornitore deve supportare l'Amministrazione nell'esecuzione di una prova di collaudo "sul campo" atta a verificare la conformità delle caratteristiche di ogni singolo servizio contrattualizzato dall'Amministrazione:

- alle indicazioni contenute nel "Piano dei fabbisogni" redatto dalla singola Amministrazione;
- al progetto del Fornitore descritto nel "Progetto dei fabbisogni";
- alle specifiche contenute nel presente Capitolato Tecnico;
- ai risultati delle verifiche effettuate per la Certificazione del Servizio.

[RR.170] Il Fornitore deve consegnare all'Amministrazione un documento intitolato "*Specifiche di dettaglio delle prove di collaudo*" che descrive la tipologia delle prove di collaudo previste e la pianificazione temporale delle stesse. Questo documento deve essere approvato dall'Amministrazione.

[R.404] Le prove di collaudo devono verificare almeno:

- caratteristiche HW/SW e funzionalità dei sistemi installati;
- connettività end-to-end, se prevista dal servizio;
- servizi di sicurezza implementati;
- rilevazioni sugli indicatori di qualità del servizio;
- procedure di fatturazione e rendicontazione.

[R.405] Il Fornitore deve altresì impegnarsi, qualora richiesto dall'Amministrazione, a svolgere ulteriori prove integrative. L'Amministrazione può procedere, a sua discrezione, ad un collaudo a campione.

[RR.171] Il Fornitore deve fornire a proprie spese e con espressa impossibilità di rivalersi sull'Amministrazione, mezzi, personale ed ogni altra strumentazione necessari all'esecuzione delle prove.

[RR.172] L'esito positivo del collaudo di configurazione di ciascun servizio da parte dell'Amministrazione consentirà il rilascio del servizio. La data del verbale di collaudo, congiuntamente sottoscritto dal Fornitore e dall'Amministrazione, verrà considerata quale data di accettazione ed attivazione dei servizi oggetto della fornitura. Tale data sarà considerata come l'inizio dell'erogazione dei servizi, salvo diverso accordo tra le parti sulla data di inizio dell'erogazione. Il pagamento dei corrispettivi per la fornitura dei servizi avrà decorrenza a partire dal 1° giorno del mese successivo alla data di collaudo positivo (verbale di collaudo) dei servizi.

13 DOCUMENTAZIONE DI RISCONTRO

Nel presente capitolo sono elencati i documenti che devono essere redatti e gestiti dal Fornitore.

[R.406] Il Fornitore deve inviare tutta la documentazione di seguito descritta in formato elettronico (almeno in formato .pdf). E' facoltà dei destinatari della documentazione richiedere l'invio della stessa anche in formato cartaceo.

[RR.173] Tutta la documentazione tecnica relativa ai servizi di seguito descritta deve essere conforme alla norma UNI EN ISO 9004-2 ed in particolare deve contenere:

- le *specifiche del servizio* comprendenti:
  - una chiara descrizione delle caratteristiche del servizio soggette a valutazione del cliente;
  - le condizioni di accettabilità per ciascuna caratteristica del servizio;
- le *specifiche di realizzazione del servizio*, comprendenti:
  - chiara descrizione delle caratteristiche di realizzazione del servizio che influenzano direttamente le prestazioni del servizio;
  - le condizioni di accettabilità per ciascuna caratteristica di realizzazione del servizio;
  - i requisiti delle risorse (hw, sw ed umane, in quest'ultimo caso la quantità ed il profilo professionale) utilizzate per svolgere il servizio;
- le *specifiche di controllo qualità del servizio*, comprendenti la definizione dei metodi di valutazione e controllo delle caratteristiche e della realizzazione dei servizi;
- le *specifiche di dettaglio delle prove di collaudo del servizio*, comprendenti la descrizione dell'ambiente di prova e l'elenco delle prove di collaudo.

13.1 Documentazione relativa al Contratto Quadro

[RR.174] L'elenco della documentazione di riscontro che deve essere predisposta dal Fornitore in relazione alla propria struttura amministrativa e tecnica per l'erogazione dei servizi della CN RUPAR-SPC è riportato nella tabella seguente con l'indicazione, per ciascun documento, dei contenuti di particolare interesse da articolare nelle tre tipologie di documento indicate nel requisito [RR.173]:

Documento di riscontro	Contenuto	Rif.	Disponibilità temporale	Destinatario
Documento programmatico di gestione della sicurezza	• Descrizione delle misure organizzative (ruoli, responsabilità e procedure), tecniche (sistemi hw e sw impiegati) e fisiche adottate.	N.A.	Entro novanta (90) giorni dalla data di sottoscrizione del Contratto Quadro	InnovaPuglia S.p.A.

Piano generale per l'erogazione dei servizi	• Descrizione della struttura funzionale ed organizzativa del Fornitore ai fini dell'erogazione dei servizi oggetto della presente gara. • Matrice compiti-responsabilità. • Pianificazione delle macro attività necessarie per la realizzazione delle infrastrutture e l'erogazione dei servizi.	N.A.	Entro novanta (90) giorni dalla data di sottoscrizione del Contratto Quadro	InnovaPuglia S.p.A.
Documentazione tecnica relativa ai Servizi di Gestione e Manutenzione	• Descrizione architetturale e funzionale del NOC/SOC. • Numero, tipologia e caratteristiche tecniche dell'hardware utilizzato per erogare il servizio. • Tipologia e release del software utilizzato per erogare il servizio. • Caratteristiche dei collegamenti tra la rete del Fornitore ed i sistemi utilizzati per erogare il servizio. • Caratteristiche architetturali, tecniche e funzionali del sito web, con descrizione della modalità con cui verrà gestito. • Caratteristiche tecniche dei sistemi utilizzati per il call center, e criteri di dimensionamento delle risorse umane ad esso dedicate.	§ 9	Entro novanta (90) giorni dalla data di sottoscrizione del Contratto Quadro	InnovaPuglia S.p.A.

Documentazione tecnica relativa ai Servizi di Interazione con le Infrastrutture Condivise	• Descrizione dell'infrastruttura di rete utilizzata per l'erogazione dei servizi. • Caratteristiche degli apparati di interconnessione presenti nei locali di EPO: – Dimensioni di ingombro degli apparati e spazi complessivi necessari, comprese le aree di disimpegno per un'agevole ispezionabilità. – Assorbimento di potenza misurato in kVA. – Caratteristiche del collegamento di terra necessario al corretto funzionamento dei sistemi. – Presenza eventuale del gruppo di continuità e di batterie e accumulatori. – Necessità o meno di condizionamento ambientale o di ventilazione forzata, indicando la dissipazione energetica. – Limiti di temperatura e di umidità relativa sopportati. – Modalità di interconnessione tra le parti, con indicazione di necessità o meno di pavimento sopraelevato. • Meccanismi/protocolli utilizzati per realizzare l'integrazione tra la rete del FSR e le infrastrutture condivise.	§ 10	Entro novanta (90) giorni dalla data di sottoscrizione del Contratto Quadro	InnovaPuglia S.p.A.

Documentazione tecnica relativa all'erogazione dei Servizi di Trasporto Dati	• Caratteristiche degli apparati di terminazione dei servizi presso le sedi dell'Amministrazione: – Dimensioni di ingombro degli apparati e spazi complessivi necessari, comprese le aree di disimpegno per un'agevole ispezionabilità. – Assorbimento di potenza misurato in kVA. – Caratteristiche del collegamento di terra necessario al corretto funzionamento dei sistemi. – Presenza eventuale del gruppo di continuità e di batterie e accumulatori. – Necessità o meno di condizionamento ambientale o di ventilazione forzata, indicando la dissipazione energetica. – Limiti di temperatura e di umidità relativa sopportati. – Modalità di interconnessione tra le parti, con indicazione di necessità o meno di pavimento sopraelevato. • Caratteristiche architetturali e tecnologiche degli accessi utilizzati (wired e wireless). • Descrizione dell'infrastruttura di rete utilizzata per l'erogazione dei servizi.	§ 4	Contestualmente all'invio del rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione del servizio	InnovaPuglia S.p.A. e Amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa alla funzionalità DNS	• Numero, tipologia e caratteristiche tecniche dell'hardware utilizzato per erogare il servizio. • Tipologia e release del software utilizzato per erogare il servizio.	§ 4	Contestualmente all'invio del primo rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione di un Servizio di Trasporto Dati	InnovaPuglia S.p.A. e Amministrazioni che acquisiscono il Servizio di Trasporto Dati
Documentazione tecnica relativa all'erogazione del Servizio di Posta Elettronica	• Numero, tipo e caratteristiche tecniche dei sistemi hardware utilizzati per erogare il servizio. • Tipologia e release del software utilizzato per erogare il servizio. • Caratteristiche dei collegamenti tra la rete del FSR ed i sistemi utilizzati per erogare il servizio.	§ 5	Contestualmente all'invio del rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione dello specifico servizio	InnovaPuglia S.p.A. e Amministrazioni che acquisiscono il servizio

Documentazione tecnica relativa ai Servizi di Sicurezza	• Numero, tipologia e caratteristiche tecniche dell'hardware utilizzato per erogare il servizio. • Tipologia e release del software utilizzato per erogare il servizio. • Caratteristiche dei collegamenti tra la rete del Fornitore ed i sistemi utilizzati per erogare il servizio. • Meccanismi/protocolli utilizzati per realizzare l'integrazione con altri strumenti di sicurezza forniti dal Fornitore o da terzi, la modalità e il livello di integrazione.	§ 6	Contestualmente all'invio del rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione dello specifico servizio	InnovaPuglia S.p.A. e Amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa ai Servizi di Comunicazione Evoluta	• Descrizione delle soluzioni architetturali richieste. • Tipologia e caratteristiche tecniche dei sistemi hardware e software utilizzati per erogare il servizio. • Descrizione delle modalità di interfacciamento con la rete PSTN. • Protocolli utilizzati per la fornitura del servizio ed ulteriori protocolli supportati dalle apparecchiature.	§ [RR.97]	Contestualmente all'invio del rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione dello specifico servizio	InnovaPuglia S.p.A. e Amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa ai Servizi di Supporto Professionale	• Curriculum Vitae dei professionisti coinvolti • Certificazioni dei professionisti coinvolti • Piano dei corsi di formazione	§ 8	Contestualmente all'invio del rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione dello specifico servizio	InnovaPuglia S.p.A. e Amministrazioni che acquisiscono il servizio
Specifiche di dettaglio delle prove di collaudo dei servizi	• Descrizione dell'ambiente di prova • Elenco delle prove di Collaudo	§ 12.2	Contestualmente all'invio del rapporto di lavoro che sancisce l'ultimazione delle attività propedeutiche all'erogazione dello specifico servizio	InnovaPuglia S.p.A.

13.2 Documentazione relativa al Contratto Esecutivo

Documento di riscontro	Contenuto	Rif.	Destinatario
Progetto dei fabbisogni	• Descrizione della nuova rete della Amministrazione. • Piani di indirizzamento delle Amministrazioni. • Regole di traduzione di indirizzi (NAT). • Dimensionamento dei servizi/accessi. • Modalità di attivazione dei servizi.	§ 11	Amministrazioni
Progetto di attuazione (parte integrante del Documento "Progetto dei fabbisogni")	• Dettaglio dei costi del progetto	§ 11	Amministrazioni
Modalità di presentazione e approvazione degli Stati di Avanzamento Mensili (parte integrante del Documento "Progetto dei fabbisogni")	• Formato degli Stati di Avanzamento o Servizi installati. o Esito dei collaudi effettuati. o Collaudi previsti nel mese successivo. o Varianti e modifiche emerse nel periodo. o Ritardi verificatisi nelle attivazioni rispetto alle date previste nel Piano di Attuazione e cause. o Penali dovute per ritardi.	§ 11	Amministrazioni
Piano di Attuazione (parte integrante del Documento "Progetto dei fabbisogni")	• Descrizione della struttura funzionale ed organizzativa del Fornitore ai fini dell'erogazione dei servizi oggetto del Piano di Attuazione. • Descrizione delle procedure di attivazione dei servizi e piano di installazione. • Matrice compiti-responsabilità. • Risorse allocate. • Specifiche di realizzazione dei servizi. • Identificazione delle attività (procedure di provisioning delle linee TLC, apparati, ecc.) necessarie all'attivazione dei servizi. • Identificazione dei rischi e piano di recovery: fasi di verifica e riesame per l'individuazione di eventuali criticità insorte nonché riferimento alle procedure necessarie alla gestione/superamento delle stesse.	§ 11	Amministrazioni
Piano Operativo (parte integrante del Documento "Piano di Attuazione")	• Pianificazione temporale dettagliata (diagramma di Gantt delle singole attivazioni, • schedulazione delle milestone principali, piano dei sopralluoghi, ecc.).	§ 11	Amministrazioni
Documento programmatico di gestione della sicurezza dell'Amministrazione (parte integrante del Documento "Piano di Attuazione")	• Descrizione delle misure organizzative (ruoli, responsabilità e procedure), tecniche (sistemi hw e sw impiegati) e fisiche adottate dal Fornitore in fase di erogazione dei servizi richiesti dall'Amministrazione.	§ 11	Amministrazioni

Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi (parte integrante del Documento "Piano di Attuazione")	• Specifiche dei servizi che descrivono in dettaglio le caratteristiche tecniche delle singole tipologie di servizio e le condizioni di accettabilità per ciascuna caratteristica. • Specifiche di realizzazione dei servizi, che descrivono le modalità di realizzazione ed erogazione del servizio e le risorse necessarie (modalità di provisioning, caratteristiche tecniche/dimensionali degli apparati utilizzati, requisiti elettrici, fisici ed ambientali che devono essere previsti nelle sedi dell'Amministrazione che ospita i servizi, nonché il modeling della rete). • Obiettivi di qualità, espressi in termini di livelli di servizio. • Metriche per la misura della qualità effettivamente fornita. • Identificazione dei controlli (test, reviews, verifiche, validazioni) che il Fornitore svolge per assicurare la qualità della fornitura ed i relativi piani di verifica. • Specifiche responsabilità riguardo ai controlli da svolgere e riguardo alla gestione dei problemi ed alla gestione delle non conformità. • Metodi, tecniche, strumenti, risorse, competenze previste dal Fornitore per assicurare la qualità della fornitura in corso d'opera. • Documenti prodotti dal sistema di assicurazione e controllo qualità. • Documenti di riferimento (guide, procedure, moduli, checklist, ecc.) utilizzati dal sistema di assicurazione e controllo qualità.	§ 11	Amministrazioni
Specifiche di dettaglio delle prove di collaudo	• Tipologia di collaudo. • Elenco delle prove di collaudo. • Tempi dei collaudi.	§ 12.3	Amministrazioni