Centro Nazionale per l'informatica nella Pubblica Amministrazione

Allegato 2b alla lettera d'invito

CAPITOLATO TECNICO

GARA A LICITAZIONE PRIVATA PER L'APPALTO DEI

SERVIZI DI CONNETTIVITÀ E SICUREZZA

NELL'AMBITO DEL SISTEMA PUBBLICO DI CONNETTIVITA'

INDICE

PREMESSA

Il presente Documento formula le modalità ed i requisiti tecnici minimi del **Sistema Pubblico di Connettività (SPC)** limitatamente alla:

- fornitura dei servizi di **connettività**,
- fornitura dei servizi di **sicurezza**,
- realizzazione e gestione della **rete di interconnessione** tra le reti dei fornitori assegnatari, denominata **Qualified eXchange Network (QXN)**.

Il presente Capitolato Tecnico si compone di:

- una **prima parte**, che descrive l'oggetto della fornitura, costituita da due sezioni:
  - ***sezione I*** (capitoli da 1 a 5), contenente la descrizione delle caratteristiche tecniche dei servizi e delle modalità di erogazione degli stessi da parte di ciascun fornitore assegnatario;
  - ***sezione II*** (capitolo 6), contenente la descrizione delle modalità con cui dovrà essere realizzata e gestita da tutti i fornitori assegnatari la QXN (cfr. Lettera d'Invito ed allegato 4) nonché delle caratteristiche dei servizi che essa dovrà erogare.
- una **seconda parte** (capitoli da 7 a 8), che descrive le procedure di collaudo previste e la documentazione di riscontro che dovrà essere consegnata alle amministrazioni ed al CNIPA.

Di seguito il concorrente primo nella graduatoria definitiva sarà denominato fornitore aggiudicatario, tutti i concorrenti a cui sarà affidata la fornitura di una delle parti dell'appalto, ivi compreso il fornitore aggiudicatario, saranno denominati fornitori assegnatari.

PARTE PRIMA - OGGETTO DELLA FORNITURA

SEZIONE I – SERVIZI EROGATI DAL FORNITORE ASSEGNATARIO

1 SERVIZI DI CONNETTIVITA'

1.1 Servizi di trasporto

I servizi di trasporto, ovvero quelli dedicati alla trasmissione di dati, **inclusi immagini e fonia**, dovranno essere basati sul protocollo IP e conformi alle normative di riferimento IETF applicabili.

I servizi di trasporto dovranno permettere potenzialmente ad ogni amministrazione la trasmissione/ricezione di pacchetti IP verso/da tre diverse tipologie di ambito:

- **Intranet**: un ambito costituito dal dominio interno alla singola amministrazione che connette tutte le sedi della stessa distribuite sul territorio;
- **Infranet**: un ambito di interconnessione che connette tra loro le singole amministrazioni sia assegnate allo stesso fornitore che, tramite la QXN, a fornitori diversi;
- **Internet**: un ambito di interazione tra le singole amministrazioni e gli utenti esterni ad esse fruitori dei servizi erogati dalle stesse.

I collegamenti fra le sedi di una o più amministrazioni (Intranet/Infranet) dovranno essere generalmente realizzati in Virtual Private Network (VPN) per lo scambio di traffico IP solo tra sedi appartenenti ad un medesimo gruppo chiuso; all’interno di una VPN dovranno poter essere definiti, se richiesti delle amministrazioni, anche dei "sottogruppi chiusi di accessi".

Per consentire la comunicazione tra le reti, i fornitori assegnatari dovranno connettersi alla QXN attraverso collegamenti ad almeno due nodi della QXN stessa. In ciascun nodo, sulla LAN realizzata per il peering, ogni fornitore SPC dovrà installare a suo carico almeno due Border Router e su questi sarà convogliato tutto il traffico proveniente dal SPC da e per le amministrazioni attestate sulla propria rete.

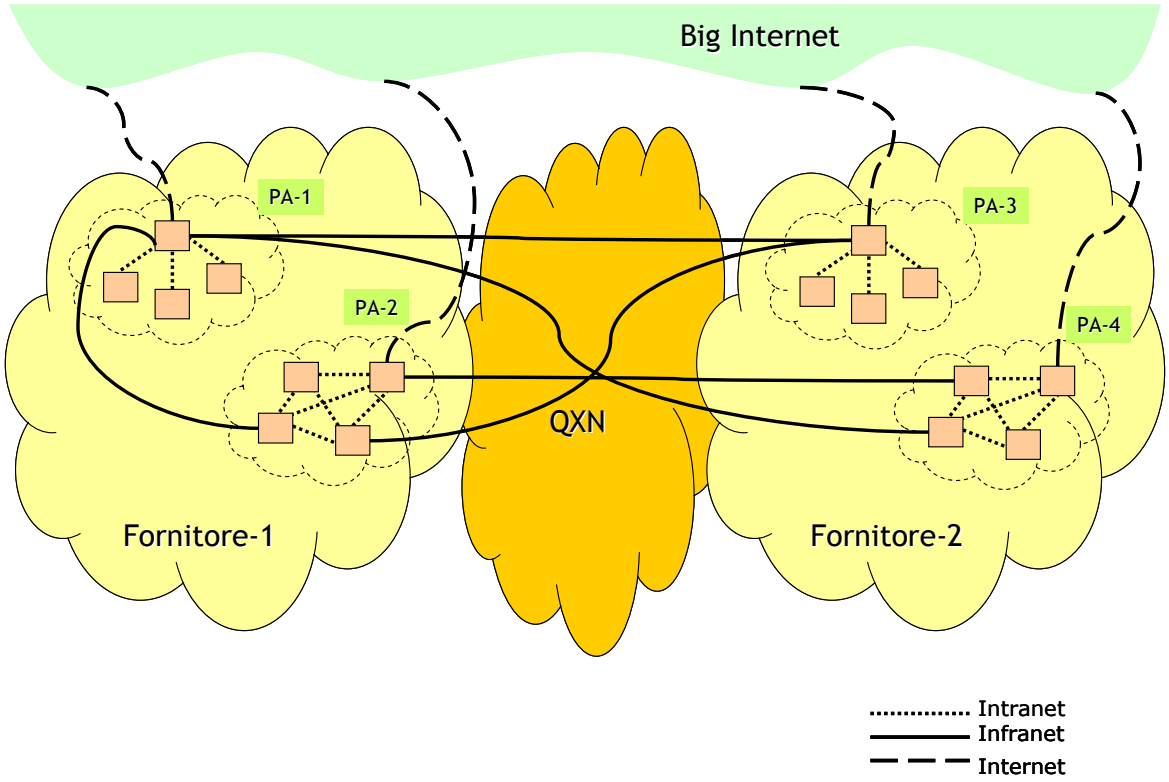

Figura 1: Esempi di collegamenti fra amministrazioni

I servizi di trasporto abilitano le amministrazioni ad usufruire di tutte le funzionalità tipiche delle reti IP. A tal fine i fornitori assegnatari dovranno assicurare il trasporto di tutti i protocolli veicolabili su IP, salvo le eventuali limitazioni imposte dai vincoli di sicurezza riportati nel paragrafo 1.5.2 .

I servizi di trasporto dovranno fornire le prestazioni minime definite negli allegati 2c e, ove applicabile, 3a.

I servizi di trasporto saranno caratterizzati da parametri oggettivi indipendenti dalle infrastrutture tecnologiche utilizzate per l'erogazione, permettendo di ottenere l'equivalenza dei servizi pur lasciando alla scelta del fornitore assegnatario la libertà tecnologica. Il fornitore assegnatario dovrà comunque essere disponibile, di concerto con il CNIPA e conformemente con la normativa in vigore, ad adottare nuove tecnologie eventualmente disponibili in futuro per i servizi offerti e per l'introduzione di nuovi servizi.

I servizi di trasporto permettono il collegamento alla rete fissa del fornitore assegnatario secondo le seguenti modalità:

- **"always-on":** mediante tecnologie che consentono accessi permanenti (ad esempio xDSL, SDH, etc.);
- **"dial-up":** mediante tecnologie che consentono accessi a commutazione di circuito PSTN, ISDN;

- **“wireless”:** mediante tecnologie che consentono accessi basati su trasmissioni in radio frequenza.

I servizi di trasporto del fornitore assegnatario dovranno essere in grado di garantire caratteristiche differenziate per il trasferimento dei pacchetti IP, in funzione delle applicazioni trasportate, secondo le seguenti quattro diverse Classi di Servizio (CdS):

- Servizi standard:
  - **IP Best Effort**: per applicazioni a bassa priorità;
  - **IP Mission Critical**: per applicazioni che richiedono il trasporto di dati critici ad alta priorità;
- Servizi real time:
  - **IP Streaming**: per applicazioni audio-video streaming a bassa interattività ed alto buffering;
  - **IP Real Time**: per applicazioni che trasportano voce su IP e per applicazioni audio-video streaming ad alta interattività e basso buffering.

A seconda delle modalità di trasporto scelte, potranno essere disponibili una o più CdS come specificato nei paragrafi da 1.1.1 a 1.1.3 .

I pacchetti IP appartenenti a diverse CdS saranno marchiati dall’amministrazione attraverso l’inserimento di opportuni valori nel campo ToS (Type of Service) dell’intestazione IP del pacchetto, secondo le specifiche che verranno stabilite dal Comitato di Direzione Tecnica di cui all’art. 15.8 del Contratto Quadro OPA. All’interno della propria rete il fornitore potrà mappare le quattro classi di servizio sulle proprie, purché garantisca il mantenimento della corretta marchiatura dei pacchetti sull’interfaccia tra la propria rete e tutte le altre reti facenti parte del SPC.

Per ogni servizio di trasporto, il fornitore dovrà provvedere, a richiesta dell’amministrazione, a marchiare i pacchetti sull’apparato che realizza l’interfaccia di punto d’accesso al servizio secondo politiche basate sull’indirizzo IP di origine, sull’indirizzo IP di destinazione, sul protocollo applicativo utilizzato o una combinazione di questi.

1.1.1 Servizi di trasporto always-on

I servizi IP always-on dovranno permettere all’amministrazione la trasmissione/ricezione di pacchetti IP nei tre ambiti (Intranet, Infranet, Internet) o ad un sottoinsieme di questi indicato dall’amministrazione.

Ogni servizio erogato sarà caratterizzato da una o più interfacce fisiche lato utente definite come Punto di Accesso al Servizio (PAS).

Ogni servizio di trasporto always-on è definito da due tipi di componenti caratterizzati da diversi parametri che il fornitore dovrà rispettare.

I due tipi di componenti sono:

- **Componente di Accesso (CdA)**, che caratterizza il collegamento utilizzato per connettere una sede dell’amministrazione con il SPC.
- **Componente di Trasferimento (CdT)**, che caratterizza le garanzie di prestazioni fornite per i differenti tipi di traffico.

Ad ogni servizio di trasporto always-on saranno associati un PAS, una componente di accesso ed una o più componenti di trasferimento.

I parametri del servizio che caratterizzano la componente di accesso e le singole componenti di trasferimento sono:

- Per la **CdA**:
  - Banda Massima in Accesso
  - Terminazione di rete
  - Livello di affidabilità
- Per la **CdT**:
  - Ambito
  - Classe di Servizio
  - Banda Garantita in Accesso o Banda Garantita End-To-End

La descrizione delle grandezze e dei parametri (disponibilità, banda garantita, tempi di ritardo, affidabilità) delle componenti è sempre definita intendendo come PAS l'interfaccia interna (ovvero quella d'utente) dell'apparato di accesso.

Componente di accesso dei servizi di trasporto always-on

Banda Massima in Accesso (BMA)

La BMA rappresenta il massimo valore della banda che il fornitore assegnatario renderà disponibile su un determinato accesso ed è descritta da un valore per la direzione Upstream (BMA_u) e da un valore per la direzione Downstream (BMA_d). Un accesso potrà essere asimmetrico (ossia $BMA_u<BMA_d$) o simmetrico (ossia $BMA=BMA_u= BMA_d$).

Per ogni accesso il fornitore dovrà assicurare le seguenti 3 condizioni:

- l'accesso dovrà supportare flussi di traffico con qualsiasi valore di Banda Garantita, purché la somma delle bande garantite sia inferiore od uguale alla BMA;
- la rete dovrà rendere possibile, almeno in alcuni momenti, l'utilizzo dell'intera banda fisica di accesso. Il fornitore assegnatario pertanto, non potrà utilizzare politiche di traffic shaping sulla Terminazione di Rete che impediscano all'utente, in assenza di congestione di rete, di arrivare ad utilizzare l'intera banda fisica di accesso.
- Per ogni BMA la banda fisica disponibile sull'accesso non dovrà inferiore almeno a quanto riportato nella seguente tabella 1;

Il fornitore dovrà fornire accessi con i valori di BMA elencati nella tabella successiva. I valori di BMA simmetrici saranno organizzati in 3 fasce distinte in funzione dell'ordine di grandezza.

Simmetrico						Asimetrico			
Fascia 1		Fascia 2		Fascia 3		BMA		Banda Fisica	
BMA	Banda Fisica	BMA	Banda Fisica	BMA	Banda Fisica	Down	Up	Down	Up
50	***64***	***2.000***	***4096***	***100.000***	***100.000***	***600***	***100***	***640***	***128***
100	***128***	***4.000***	***8192***	***200.000***	***200.000***	***600***	***250***	***640***	***256***
200	***256***	***8.000***	***10.000***	***300.000***	***300.000***	***1000***	***250***	***1280***	***256***
300	***384***	***10.000***	***10.000***	***600.000***	***600.000***	***1600***	***500***	***2048***	***512***
400	***512***	***20.000***	***20.000***	***1.000.000***	***1.000.000***				
500	***768***	***30.000***	***30.000***	***2.500.000***	***2.500.000***				
1000	***2048***	***60.000***	***60.000***						

Tabella 1: Valori di Banda Massima in Accesso

Terminazione di Rete (TdR)

Il fornitore dovrà erogare il servizio di trasporto IP alle amministrazioni attraverso l'impiego di un idoneo apparato di accesso che metta a disposizione dell'amministrazione l'interfaccia PAS. Tale apparato, definito TdR, dovrà essere messo a disposizione, gestito e configurato dal fornitore assegnatario come componente integrale del servizio.

Il fornitore assegnatario dovrà garantire l'accesso in lettura alla Management Information Base (MIB) delle TdR al CG-SPC e, a richiesta dell'amministrazione, alle postazioni di monitoraggio fornite all'amministrazione stessa (cfr. paragrafo 1.5.1). Le modalità di accesso alle MIB verranno definite dal CNIPA in modo tale da garantire la non interferenza con le prestazioni contrattualizzate per il servizio.

Le TdR dovranno essere allo stato dell'arte della tecnologia e del mercato, dovranno implementare protocolli allo stato dell'arte e dovranno essere dimensionate in modo da garantire il rispetto dei livelli di servizio previsti per il servizio di traporto always-on (cfr. allegati 2c e 3a).

I PAS messi a disposizione dalle TdR dovranno essere conformi allo standard Fast Ethernet (10/100 Autosensitive). Per gli accessi simmetrici di fascia 3 le TdR dovranno essere dotate di PAS realizzati da interfacce multiple Fast Ethernet o da interfacce Gigabit Ethernet (1 Gb/s), a scelta dell'amministrazione.

Per ogni valore di BMA il fornitore assegnatario dovrà fornire, inclusa nel prezzo dell'accesso una TdR di tipo **Base.** Per accessi con Livello di Affidabilità L3. L4 o L5, l'amministrazione potrà richiedere una Tdr **High Performance**, differenziata a seconda della capacità di elaborazione di pacchetti al secondo (pps).

Il fornitore dovrà garantire, a seconda della BMA degli accessi, le prestazioni minime della TdR elencate nella seguente tabella.

Collegamenti (BMA)	Capacità di gestione di pacchetti al secondo per TdR Base	Capacità di gestione di pacchetti al secondo per TdR High Performance
Asimmetrici:		**20 kpps**
1.000/250 Kb/s	2,5 kpps	
1.600/500 Kb/s	4 kpps	
Simmetrici:		
1 Mb/s	4 kpps	
2 Mb/s	6,5 kpps	
4 Mb/s	12 kpps	
8 Mb/s	22,5 kpps	**200 kpps**
10 Mb/s	30 kpps	
20 Mb/s	50 kpps	
30 Mb/s	75 kpps	
60 Mb/s	140 kpps	
100 Mb/s	220 kpps	**2.000 kpps**
200 Mb/s	420 kpps	
300 Mb/s	600 kpps	
600 Mb/s	1100 kpps	
1 Gb/s	1500 kpps	
2,5 Gb/s	1500 kpps	

Tabella 2: Pacchetti al secondo gestiti dalle TdR

Nel caso in cui l'amministrazione richieda 2 o più servizi always-on all'interno della stessa sede dotati di TdR High Performance, il fornitore assegnatario dovrà, a richiesta dell'amministrazione, provvedere al collegamento delle TdR con prestazioni di **bilanciamento di carico**.

Livelli di affidabilità

Per ogni accesso il fornitore assegnatario dovrà garantire, a scelta dell'amministrazione, uno dei cinque possibili livelli di affidabilità definiti nella seguente tabella. Per la definizione dei singoli parametri e dei valori possibili si rimanda agli allegati 2c e 3a.

Livelli di Affidabilità / Parametro	L1	L2	L3	L4	L5
Disponibilità unitaria	Base	Base	Standard	Standard	Mission Critical
Tempo di ripristino	Base	Standard	Standard	Veloce	Veloce
Finestra di erogazione	Standard	Standard / Estesa	Standard / Estesa	Standard / Estesa	Estesa

Tabella 3: Livelli di affidabilità contrattualizzabili

Il fornitore dovrà assicurare, attraverso opportune misure tecnico-organizzative (ad es. ridondanza dell'infrastruttura fisica di accesso, back-up, ridondanza degli apparati di accesso, presidi tecnici presso il cliente) il rispetto dei valori di disponibilità unitaria dell'accesso, tempo di ripristino, ripetitività dei disservizi e finestra temporale di erogazione definiti negli allegati 2c e 3a.

Componente di trasferimento dei servizi di trasporto always-on

Ambito

Le componenti di trasporto erogate dal fornitore assegnatario dovranno consentire l'accesso ai 3 ambiti definiti nel paragrafo 1.1 (Intranet, Infranet, Internet).

Una singola componente di trasferimento sarà caratterizzata da un solo ambito; differenti componenti di trasferimento associate ad una stessa componente di accesso potranno essere caratterizzate da differenti ambiti.

Classe di servizio (CdS)

La CdS viene identificata dai seguenti parametri di rete:

- **Ritardo di trasferimento**: tempo necessario ad un pacchetto IP per un tragitto end-to-end. In funzione della CdS la misura di tale parametro farà riferimento alla tratta origine-destinazione (One-Way Delay, OWD) o alla tratta origine-destinazione-origine (Round Trip Delay, RTD).
- **Tasso di perdita dei pacchetti**: percentuale di pacchetti trasmessi, ma non consegnati.
- **Jitter**: deviazione standard del OWD di trasferimento dei pacchetti.

Nella Tabella 4 sono riportati i valori delle soglie dei parametri di qualità della rete che il fornitore dovrà assicurare per ciascuna CdS tra accessi di tipo always-on:

	Ritardo di trasferimento round trip (RTD) o one-way (OWD)	**Tasso di perdita dei pacchetti**	**Jitter (OWD)**
IP Best Effort	RTD < 500 ms	< 5%	-
IP Mission Critical	RTD < 100 ms	< 0,1%	-
IP Streaming	OWD < 400 ms	< 0,5%	250 ms
IP Real time	OWD < 40 ms	< 0,1%	10 ms

Tabella 4: Classificazione dei servizi di connettività

Le modalità di misura dei parametri sopra elencati sono descritte negli allegati 2c e 3a.

Per ciascuna CdT il fornitore assegnatario dovrà rendere disponibili le seguenti opzioni:

- per l'ambito Intranet, una delle 4 CdS a scelta dell'amministrazione;
- per l'ambito Infranet, una delle 4 CdS a scelta dell'amministrazione;
- per l'ambito Internet, la sola CdS IP Best Effort.

Garanzie di banda

Per ciascuna CdT, oltre alle prestazioni relative alla CdS, il fornitore dovrà garantire una Banda Garantita in Accesso (BGA) o in alternativa una Banda Garantita End-To-End (BGETE), definita come segue:

- **BGA**: si intende la velocità in trasmissione e/o ricezione fino alla quale la rete dovrà garantire il trasporto con il rispetto dei parametri di qualità definiti per ciascuna CdS. La banda sarà garantita solo sulla tratta di accesso; in ogni caso il fornitore dovrà dimensionare la propria rete in modo da assicurare il rispetto dei parametri all'interno della rete stessa secondo quanto definito dagli SLA negli allegati 2c e 3a.
- **BGETE**: si intende la velocità in trasmissione e/o ricezione fino alla quale dovrà essere garantito il trasporto dei dati, con il rispetto dei parametri di qualità definiti per la CdS in oggetto, sull'intero percorso all'interno della rete del fornitore.

Per ogni CdT il fornitore assegnatario dovrà rendere disponibili valori di BGA o BGETE compresi fra 10 Kb/s e 2,5 Gb/s con granularità di 10 Kb/s, fermo restando la limitazione della Banda Garantita totale su una CdA.

Disponibilità geografica dei servizi di trasporto always-on

Il fornitore assegnatario dovrà erogare servizi di trasporto always-on con la seguente disponibilità geografica:

- i servizi asimmetrici, con copertura almeno coincidente con quella del servizio ADSL wholesale di Telecom Italia;
- i servizi simmetrici con BMA inferiore a 2 Mb/s, ovunque sul territorio nazionale;
- i servizi simmetrici con BMA maggiore od uguale a 2 Mb/s e inferiore a 10 Mb/s, almeno in tutti i comuni capoluogo di provincia;
- i servizi simmetrici con BMA maggiore od uguale a 10 Mb/s e fino a 100 Mb/s (inclusi), almeno all'interno dei comuni capoluogo di regione, inclusi i comuni sede di provincia autonoma di Trento e Bolzano;
- i servizi con BMA superiore a 100 Mb/s, almeno all'interno dei comuni di Roma e Milano.

1.1.2 Servizi di trasporto dial-up

Il fornitore dovrà erogare servizi dial-up che consentano l'accesso a VPN-IP da parte di un singolo PC tramite linee telefoniche analogiche (PSTN) o digitali (ISDN). La configurazione della stazione di lavoro, o di eventuali apparati di accesso, sarà responsabilità dell'amministrazione.

Il fornitore assegnatario dovrà erogare i servizi dial-up su tutto il territorio nazionale.

Per i servizi di trasporto dial up, il PAS è definico come linterfaccia del router che implementa la porta modem attestata sulla rete telefonica su cui terminano le chiamate telefoniche.

Ogni servizio di trasporto dial-up sarà definito dalle seguenti di componenti:

- **Componente di Accesso (CdA),** che costituisce la modalità di connessione al SPC;
- **Componente di Terminazione del Traffico (CTT)**, che costituisce una caratterizzazione di garanzie di prestazioni fornite per la terminazione del traffico;
- **Componente di Autenticazione, Autorizzazione ed Accounting (AAA)**.

Componente di accesso

La **connessione analogica** (da PSTN) dovrà supportare i seguenti standard:

- V21, V22, V22bis, V32, V32bis, V34, V34bis, K56Flex, V90, V92;
- V42, MNP4 (correzione dell'errore);
- V42bis, MNP5 (compressione dei dati).

La **connessione da rete ISDN** dovrà avvenire almeno con un canale B (64 Kb/s) conformemente allo standard ETSI 300 102. Il servizio IP di tipo commutato dovrà essere basato sul protocollo PPP (RFC 1661) e, nel caso di utilizzo contemporaneo di più canali B ISDN, dovrà essere supportato il protocollo Multilink PPP (RFC 1717 e seguenti).

Il fornitore dovrà rendere disponibili due modalità di fornitura degli accessi dial-up:

- **Accesso nominale su base User-Id (NOM)**. L'amministrazione contrattualizzerà il numero massimo di username a cui il fornitore assegnatario dovrà garantire l'accesso alla rete. Il dimensionamento delle porte e dell'infrastruttura di rete dovranno garantire a ciascuna amministrazione la possibilità di impiego del servizio in termini di tasso di occupato in modo da rispettare gli SLA (cfr. allegati 2c e 3a).
- **Accesso su base Porta Virtuale (VIR)**. L'amministrazione contrattualizzerà un numero massimo di porte virtualizzate su tutto il territorio nazionale, corrispondenti al numero di utenti contemporaneamente connessi in rete. Una ulteriore richiesta di connessione da parte di un utente, una volta raggiunto il numero massimo consentito, verrà rifiutata dalla rete. In questo caso l'amministrazione definirà le proprie utenze senza nessun vincolo sul numero e sarà quindi responsabile del rapporto di concentrazione: (numero totale utenti) / (numero massimo porte virtualizzate). Il fornitore assegnatario dovrà garantire a ciascuna amministrazione la possibilità di impiego del servizio in termini di tasso di occupato quando il numero di utenti contemporaneamente connessi è minore o uguale al numero massimo di porte contrattualizzato.

Le linee telefoniche PSTN o ISDN utilizzate per accedere ai servizi dial-up saranno a carico dell'amministrazione.

Componente di Terminazione del Traffico

Il fornitore dovrà garantire che le utenze abilitate possano connettersi al SPC da tutto il territorio nazionale, indipendentemente dall'area locale o dalla rete telefonica dalla quale viene originata la chiamata, senza alcuna limitazione temporale.

Il fornitore dovrà rendere disponibile una tariffazione con un numero unico su tutto il territorio nazionale (ad es. numerazione in decade 7), con addebito a carico del chiamato, indipendente dall'area locale dalla quale proviene la chiamata. I numeri utilizzati dovranno essere dedicati per ogni amministrazione.

Il fornitore assegnatario dovrà garantire la terminazione degli accessi dial-up su uno dei due ambiti Intranet dell'amministrazione od Internet (a seconda della User-Id utilizzata) ed il trasporto della sola CdS IP Best Effort (cfr. allegati 2c e 3a). Pacchetti appartenenti a diverse CdS dovranno comunque essere trasportati ma, ai fini del rispetto degli SLA, verranno considerati alla stregua di pacchetti di CdS IP Best Effort.

Componente di Autenticazione, Autorizzazione ed Accounting

Il fornitore assegnatario dovrà rendere disponibili funzionalità di autenticazione dell'utente basate su protocollo RADIUS. Relativamente alla localizzazione ed alla gestione del Server RADIUS (intesa come piattaforma hardware e relativo software) il fornitore assegnatario dovrà rendere disponibili le seguenti opzioni:

- **Server Radius presso la sede dell'amministrazione (R.1)**. In tal caso le utenze saranno gestite in proprio dall'amministrazione in base alle indicazioni del fornitore necessarie alla configurazione del Server RADIUS. Hardware e software saranno a carico dell'amministrazione. A richiesta dell'amministrazione il fornitore dovrà erogare un corso di formazione per il personale dell'amministrazione che avrà in carico la gestione delle funzioni AAA (gestione utenze, Server RADIUS, reportistica).
- **Server Radius gestito in outsourcing presso il fornitore (R.2)**. In questo caso il fornitore dovrà mettere a disposizione dell'amministrazione una procedura operativa per creare, modificare e cancellare le singole utenze del servizio.

Nel caso in cui l'amministrazione disponga di analoga componente per altri servizi SPC, dovrà essere possibile l'utilizzo della stessa componente di servizio AAA

1.1.3 Servizi di trasporto wireless

Il fornitore assegnatario dovrà erogare servizi wireless che consentano l'accesso alle VPN-IP facenti parte dei tre ambiti definiti nel paragrafo 1.1 . Il fornitore assegnatario dovrà rendere dispoibili tali servizi attraverso sistemi di accesso che utilizzano tecnologie radio per assicurare la raggiungibilità di sedi con particolari esigenze di connettività o per il raggiungimento di utenti della pubblica amministrazione in mobilità sul territorio.

Il fornitore assegnatario dovrà erogare le quattro seguenti tipologie di servizi wireless:

- **servizi satellitari con banda di accesso dedicata;**
- **servizi satellitari con banda di accesso condivisa;**
- **servizi di accesso Wi-Fi;**
- **servizi di accesso PLMN (Public Land Mobile Network).**

Servizi satellitari con banda di accesso dedicata

Il fornitore assegnatario dovrà erogare servizi di trasporto di traffico IP attraverso connessioni satellitari bidirezionali con banda dedicata sia in upstream che in downstream.

Il fornitore dovrà prevedere all'interno del servizio la fornitura, installazione, gestione e manutenzione di tutte le infrastrutture ed apparati necessari per la realizzazione del collegamento (antenna, supporto, apparato di terminazione, cablaggi necessari per la fruizione del servizio).

L'amministrazione richiedente dovrà rendere disponibile al fornitore assegnatario, per ogni sede su cui è richiesto il servizio, una posizione per l'installazione dell'antenna ricetrasmittente che assicuri la visibilità del satellite interessato alla trasmissione.

Il fornitore assegnatario dovrà utilizzare, per la connessione dei sistemi di utente, apparati che dovranno prevedere la possibilità di interfacciare LAN o singoli PC attraverso interfacce di rete Ethernet (10 Mb/s) che saranno il PAS per il servizio. La dimensione massima per l'antenna, salvo specifica autorizzazione dell'amministrazione, dovrà essere di 240 cm (diametro).

Il fornitore assegnatario dovrà rendere disponibile su ogni accesso una capacità dedicata al collegamento tra la sede dell'amministrazione e la rete terrestre del fornitore sia per la trasmissione che per la ricezione.

I profili di servizio dovranno essere caratterizzati dalla **Banda Dedicata in Accesso (BDA)**, che potrà essere simmetrica (lo stesso valore di BDA in entrambe le direzioni) o asimmetrica (con due differenti valori di BDA per la direzione Upstream e Downstream). Le tabelle successive elencano i profili di servizio che il fornitore assegnatario dovrà fornire alle amministrazioni.

Profili di servizio	BDA
SATD_S.1	64 kb/s
SATD_S.2	128 kb/s
SATD_S.3	256 kb/s
SATD_S.4	512 kb/s
SATD_S.5	1024 kb/s

Tabella 5: Profili dei servizi stellitari con banda di accesso dedicata simmetrica

Profili di servizio	BDA	
	Downstream	Upstream
SATD_A.1	64 kb/s	32 kb/s
SATD_A.2	128 kb/s	64 kb/s
SATD_A.3	256 kb/s	64 kb/s
SATD_A.4	512 kb/s	128 kb/s
SATD_A.5	512 kb/s	256 kb/s
SATD_A.6	1024 kb/s	256 kb/s
SATD_A.7	1024 kb/s	512 kb/s
SATD_A.8	2048 kb/s	1024 kb/s

Tabella 6: Profili dei servizi stellitari con banda di accesso dedicata asimmetrica

Il collegamento tra il satellite e la rete terrestre del fornitore assegnatario e al SPC dovrà essere incluso nel servizio e dimensionato in modo tale da rispettare i parametri descritti nel presente paragrafo e da garantire gli SLA definiti negli allegati 2c e 3a.

In particolare i servizi satellitari con banda di accesso dedicata dovranno prevedere il trasporto del solo tipo di classe di servizio IP Best Effort per tutti gli ambiti definiti o, a richiesta dell'amministrazione, per un sottoinsieme di essi. Pacchetti appartenenti a diverse CdS dovranno comunque essere trasportati ma, ai fini del rispetto degli SLA, verranno considerati alla stregua di pacchetti di CdS IP Best Effort.

Il fornitore assegnatario dovrà erogare i servizi satellitari con banda di accesso dedicata su tutto il territorio nazionale.

Servizi satellitari con banda di accesso condivisa

Il fornitore assegnatario dovrà erogare servizi di trasporto di traffico IP attraverso connessioni satellitari bidirezionali con banda condivisa tra tutte le sedi dell'amministrazione abilitate all'accesso.

Il fornitore dovrà prevedere all'interno del servizio la fornitura, installazione, gestione e manutenzione di tutte le infrastrutture ed apparati necessari per la realizzazione del collegamento (antenna, supporto, apparato di terminazione, cablaggi necessari per la fruizione del servizio).

L'amministrazione richiedente dovrà rendere disponibile al fornitore assegnatario, per ogni sede su cui è richiesto il servizio, una posizione per l'installazione dell'antenna ricetrasmittente che assicuri la visibilità del satellite interessato alla trasmissione.

Il fornitore assegnatario dovrà utilizzare, per la connessione dei sistemi di utente, apparati che dovranno prevedere la possibilità di interfacciare LAN o singoli PC attraverso interfacce di rete Ethernet (10 Mb/s) che rappresenteranno il PAS del servizio. La dimensione massima per l'antenna, salvo specifica autorizzazione dell'amministrazione, dovrà essere di 240 cm (diametro).

Il fornitore dovrà rendere disponibile un'unica banda sul sistema satellitare che verrà condivisa da tutte le sedi dell'amministrazione.

I sistemi trasmissivi installati nella singola sede dell'amministrazione dovranno consentire una velocità di almeno 1024 Kb/s (trasmissione) e 2048 Kb/s (ricezione).

L'insieme degli accessi con banda satellitare condivisa sarà caratterizzato dal parametro **Banda Satellitare Condivisa (BSC)**. La BSC dovrà essere separatamente contrattualizzabile per il segmento downstream verso le stazioni e upstream dal satellite. In ognuno dei due sensi la BSC dovrà essere resa disponibile per multipli interi di 2Mb/s fino ad un massimo complessivo per amministrazione di almeno 40 Mb/s.

Il collegamento tra il satellite e la rete terrestre del fornitore assegnatario e al SPC dovrà essere incluso nel servizio e dimensionato in modo tale da rispettare i parametri descritti nel presente paragrafo e da garantire gli SLA definiti negli allegati 2c e 3a.

In particolare i servizi satellitari con banda di accesso condivisa dovranno prevedere il trasporto del solo tipo di classe di servizio IP Best Effort per tutti gli ambiti definiti o, a richiesta dell'amministrazione, per un sottoinsieme di essi. Pacchetti appartenenti a diverse CdS dovranno comunque essere trasportati ma, ai fini del rispetto degli SLA, verranno considerati alla stregua di pacchetti di CdS IP Best Effort.

Il fornitore assegnatario dovrà erogare i servizi satellitari con banda di accesso condivisa su tutto il territorio nazionale.

Servizi di accesso Wi-Fi

Il fornitore assegnatario dovrà erogare servizi di accesso wireless Wi-Fi che consentano l'accesso di singoli client su uno dei due ambiti Intranet dell'amministrazione od Internet (a seconda della User-Id utilizzata) attraverso Access Point all'interno di siti pubblici.

Il fornitore assegnatario dovrà erogare i servizi di accesso wireless Wi-Fi in **almeno 50 siti pubblici** sul territorio nazionale (ad esempio aeroporti, stazioni ferroviarie, etc.). Il fornitore aggiudicatario dovrà comunicare l'elenco dei siti su cui sarà disponibile il servizio. Gli altri fornitori assegnatari potranno designare ulteriori siti su cui si impegnano ad attivare il servizio, purché si impegnino a fornire l'accesso al servizio agli altri fornitori assegnatari, a condizioni equivalenti a quelle stabilite per l'OPO.

Il fornitore assegnatario dovrà garantire la terminazione degli accessi Wi-Fi sull'ambito Intranet dell'amministrazione ed il trasporto della sola CdS IP Best Effort (cfr. allegati 2c e 3a). Pacchetti appartenenti a diverse CdS dovranno comunque essere trasportati ma, ai fini del rispetto degli SLA, verranno considerati alla stregua di pacchetti di CdS IP Best Effort.

I servizi di accesso Wi-Fi sono definiti dalle seguenti componenti:

- **Componente di Accesso (CdA)**, che costituisce la modalità di connessione al SPC;
- **Componente di Autenticazione, Autorizzazione ed Accounting (AAA)**.

Componente di Accesso (CdA)

La connessione dovrà supportare i seguenti standard:

- 802.11b, 802.11g (accesso);
- WEP, WPA (crittografia).

L'amministrazione contrattualizzerà il numero massimo di username a cui il fornitore assegnatario dovrà garantire l'accesso alla rete su tutti gli access point.

Componente di Autenticazione, Autorizzazione ed Accounting (AAA)

Il fornitore assegnatario dovrà garantire funzionalità di autenticazione dell'utente basate su protocollo RADIUS analogamente a quanto stabilito per i servizi di trasporto di tipo dial-up (cfr. paragrafo 1.1.2).

Nel caso in cui l'amministrazione disponga di analoga componente per altri servizi SPC, dovrà essere possibile l'utilizzo della stessa componente di servizio AAA.

Servizi di accesso PLMN

Per permettere l'accesso alla Intranet dell'amministrazione da collegamenti realizzati su reti mobili pubbliche terrestri (PLMN) GPRS o UMTS contrattualizzati con operatori PLMN, il fornitore assegnatario dovrà erogare servizi di trasporto IP che permettano il trasporto tra la rete

dell'operatore PLMN di un'amministrazione e l'ambito Intranet dell'amministrazione stessa. Il PAS del servizio è costituito dall'interfaccia fisica dell'apparato del fornitore assegnatario che interfaccia la rete dell'operatore PLMN.

Il fornitore assegnatario dovrà rendere disponibili tali interfacce, presso sue sedi, almeno nei comuni di Roma e Milano.

I servizi di accesso PLMN sono definiti dalle seguenti componenti:

- **Componente di accesso (CdA)**, che costituisce la modalità di connessione del fornitore PLMN al SPC.
- **Componente di Trasferimento (CdT)**, che caratterizza le garanzie di prestazioni fornite per i differenti tipi di traffico sul collegamento tra la rete del fornitore PLMN e i PAS dell'amministrazione.
- **Componente di Autenticazione, Autorizzazione ed Accounting (AAA)**.

Componente di Accesso (CdA)

Caratterizza la velocità fisica dell'interfaccia tra la rete dell'operatore di PLMN e la rete del fornitore assegnatario. Il fornitore dovrà mettere a disposizione le interfacce elencate nella tabella successiva.

CdA		
Fascia 1 (valori in Kb/s)	**Fascia 2 (Valori in Mb/s)**	**Fascia 3 (Valori in Gb/s)**
64	10	1
128	34	2,5
256	100	
512	155	
768		
2048		

Tabella 7: Valori di Componente di Accesso

Componente di trasferimento (CdT)

Per ogni CdA potranno essere contrattualizzate più CdT. Le CdT erogate dal fornitore assegnatario sulla CdA dovranno consentire il trasferimento del traffico IP sul solo ambito Intranet dell'amministrazione. La singola CdT sarà caratterizzata da:

- una Banda Garantita in Accesso (BGA): la velocità in trasmissione e/o ricezione fino alla quale la rete dovrà garantire il trasporto con il rispetto dei parametri di qualità definiti per ciascuna CdS (cfr. allegati 2c e 3a);
- una delle 4 classi di servizio definite nel paragrafo 1.1 .

Il fornitore assegnatario dovrà rendere disponibili valori di BGA compresi fra 10 Kb/s e 2,5 Gb/s con granularità di 10 Kb/s, purché la somma dei valori di BGA di tutte le CdT contrattualizzate sulla CdA non ecceda la velocità dell'interfaccia definita per la CdA.

Componente di Autenticazione, Autorizzazione ed Accounting (AAA)

Il fornitore assegnatario dovrà garantire funzionalità di autenticazione dell'utente basate su protocollo RADIUS analogamente a quanto stabilito per i servizi di trasporto di tipo dial-up (cfr. paragrafo 1.1.2).

Nel caso in cui l'amministrazione disponga di analoga componente per altri servizi SPC, dovrà essere possibile l'utilizzo della stessa componente di servizio AAA.

1.2 Servizi di supporto

Insieme ai servizi di trasporto il fornitore assegnatario dovrà erogare i servizi di rete descritti nel presente paragrafo, dovuti senza oneri aggiuntivi e tesi alla risoluzione di problematiche di naming/addressing in ambito QXN.

1.2.1 Gestione degli indirizzi pubblici

Il piano di indirizzamento adottato nell'ambito del SPC dovrà garantire l'univocità degli indirizzi IP attribuiti ai singoli sistemi che, connessi tramite QXN, scambieranno traffico tra loro.

Gli indirizzi IP delle amministrazioni, destinati ai servizi esposti su Internet o su Infranet, dovranno essere di tipo pubblico e messi a disposizione dal fornitore assegnatario all'interno del proprio spazio di indirizzi.

Oltre a quelli eventualmente necessari per la gestione delle proprie TdR, il fornitore assegnatario dovrà rendere disponibili, a richiesta dall'amministrazione, al fine di realizzare servizi esposti su Infranet o Internet, almeno il numero di indirizzi pubblici correlato al numero complessivo di accessi SPC always-on e wireless satellitari 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 25 a 50	64
Da 51 a 100	128
Da 101 a 200	256
Oltre 200	512

Tabella 8: Indirizzi IP pubblici disponibili

Nel caso in cui il fornitore assegnatario si avvalga dell'offerta OPO, potrà richiedere al fornitore aggiudicatario il numero di indirizzi IP pubblici indicati nella tabella precedente relativi al numero di accessi always-on e wireless satellitari contrattualizzati in OPO.

In caso di richieste ulteriori, e di indisponibilità di indirizzi da parte del fornitore assegnatario, questi dovrà farsi carico di supportare l'amministrazione nell'interfacciamento con gli Enti preposti all'assegnazione di indirizzi pubblici per ottenere l'assegnazione degli indirizzi.

Per agevolare la predisposizione di servizi all'interno della rete dell'amministrazione, il fornitore assegnatario dovrà impegnarsi, qualora l'amministrazione ne faccia richiesta, a:

- fornire servizi di Network Address Translation (NAT) per consentire l'accesso a reti con indirizzamento pubblico alle amministrazioni dotate di indirizzi privati;
- configurare sulle TdR dell'amministrazione servizi di NAT statico tra gli indirizzi pubblici e quelli privati utilizzati dall'amministrazione. La riconfigurazione dei servizi di NAT statico potrà essere richiesta dalla pubblica amministrazione al fornitore assegnatario per un massimo di 2 volte per anno solare.

Nel caso in cui un'amministrazione fosse già dotata di un proprio Autonomous System (AS), il fornitore dovrà consentire l'annuncio dei propri indirizzi tramite BGP per propagarli. Nel caso in cui l'amministrazione fosse invece già dotata di reti con indirizzamento IP privato, il fornitore assegnatario dovrà, per quanto possibile, prevedere il mantenimento dell'indirizzamento attuale, utilizzando i servizi di NAT statico ed eventualmente di NAT Management (cfr. paragrafo 2.9).

Per garantire il corretto instradamento del traffico da e verso la rete di interconnessione QXN e da e verso Internet, gli indirizzi utilizzati dal fornitore assegnatario per i servizi SPC dovranno essere annunciati verso l'AS QXN e verso altri AS connessi alla rete del fornitore assegnatario secondo le regole definite dal Comitato Tecnico della SC-QXN (cfr. paragrafo 6.3.2).

1.2.2 Domain Name Service (DNS)

Il fornitore assegnatario dovrà rendere disponibile un servizio di DNS per lo spazio dei nomi interni al SPC (cfr. RFC 1035 e sue successive integrazioni ed evoluzioni quali ad esempio RFC 1122).

Il fornitore assegnatario dovrà assicurare la continuità del servizio DNS prevedendo adeguati meccanismi di "backup a caldo".

Il fornitore assegnatario dovrà erogare alle amministrazioni che lo richiedano i seguenti servizi:

- DNS primario per la risoluzione dei nomi da parte dei sistemi dell'amministrazione;
- DNS secondario;
- DNS Reverse.

Il servizio di DNS della Infranet dovrà inoltre essere collegato al DNS di riferimento per l'Italia per il collegamento ad Internet.

1.3 Servizi VoIP

Il fornitore assegnatario dovrà mettere a disposizione di ogni singola amministrazione il servizio VoIP, ossia l'erogazione dei servizi di fonia di base e supplementari su piattaforme di rete basate sul protocollo IP. La fornitura del servizio VoIP comprende la messa in opera e la gestione di un

sistema in grado di erogare le funzionalità descritte nel paragrafo 1.3.4 , rispettando gli SLA riportati negli allegati 2c e 3a, organizzato secondo le seguenti componenti:

- postazioni utente basate su tecnologia VoIP (Voice over IP);
- integrazione con la rete di fonia privata dell'amministrazione pre-esistente;
- connessione alla rete telefonica pubblica (PSTN);
- collegamento al "nodo di interconnessione VoIP" (cfr. paragrafo 1.3.2) per l'instradamento dei servizi inter-dominio e, se richiesto dall'amministrazione, di interfacciamento verso la PSTN centralizzato. Il nodo di interconnessione VoIP non costituisce oggetto della presente gara.

Il servizio offerto dal fornitore assegnatario dovrà inoltre integrarsi completamente rispetto alle infrastrutture pre-esistenti, sia per quanto riguarda la rete IP (piano di indirizzamento, presenza di Network Address Translation, presenza di proxy di livello applicativo) sia per quanto riguarda la rete di fonia privata TDM (piano di numerazione dei derivati telefonici).

Il servizio VoIP non include:

- la capacità di connettività IP necessaria al trasporto sul SPC dei flussi informativi facenti parte del servizio stesso. Ogni amministrazione dovrà invece approvvigionarsi di una capacità in accesso al SPC dimensionando opportunamente il proprio collegamento in funzione delle risorse addizionali richieste dal servizio VoIP;
- la realizzazione e la gestione delle infrastrutture di rete IP (cablaggio strutturato), fonia TDM ed alimentazione presso i siti dell'amministrazione;
- il servizio di commutazione del traffico su rete telefonica pubblica ed il relativo rilegamento trasmissivo.

Tutti gli aspetti del presente capitolato, facenti riferimento all'interlavoro con il nodo di interconnessione VoIP, dovranno essere garantiti dal fornitore solamente a seguito dell'effettiva disponibilità ed operatività del nodo di interconnesssione VoIP.

Il fornitore assegnatario dovrà inoltre adeguare, in modo continuativo, i propri servizi alle normative che la Comunità Europea rilascerà in merito ai servizi erogati mediante tecnologia VoIP senza oneri aggiuntivi per le amministrazioni.

1.3.1 Descrizione del servizio

Nel presente Documento, con il termine "dominio VoIP", si fa riferimento ad un insieme di postazioni IP native ed i relativi elementi sede della logica di controllo delle chiamate. Su richiesta dell'amministrazione, il dominio VoIP potrà contenere anche elementi di interfacciamento verso PBX telefonici in tecnologia tradizionale TDM e verso la rete telefonica pubblica.

All'interno del singolo dominio VoIP, il fornitore assegnatario dovrà prendersi carico delle seguenti attività operative:

- installazione, configurazione e gestione delle postazioni VoIP;
- installazione, configurazione e gestione di tutti gli elementi attivi facenti parte della soluzione VoIP;
- gestione del piano di numerazione;

- scambio delle informazioni di instradamento telefonico con il nodo di interconnessione VoIP;
- gestione degli allarmi;
- gestione completa di tutte le chiamate intra-dominio (cfr. paragrafo 1.3.5);
- corretto instradamento verso/da i punti di confine del dominio (cfr. paragrafo 1.3.2) delle chiamate verso/da rete interna di fonia TDM dell'amministrazione, verso/da il nodo di interconnessione VoIP, verso/da reti telefoniche pubbliche (PSTN);
- fornire il servizio di intercettazione legale all'Autorità Giudiziaria competente secondo quanto previsto dalla normativa vigente.

Tutti gli standard di riferimento sono elencati nel paragrafo 1.3.8 .

1.3.2 Descrizione dell'architettura

Ogni dominio VoIP (cfr. Figura 2) messo a disposizione dal fornitore assegnatario dovrà essere connesso al nodo di interconnessione VoIP al fine di:

- realizzare l'interconnessione con un qualunque altro dominio VoIP (anche qualora entrambi i domini fossero sotto la gestione dello stesso fornitore);
- dietro richiesta dell'amministrazione, abilitare l'interconnessione con la PSTN.

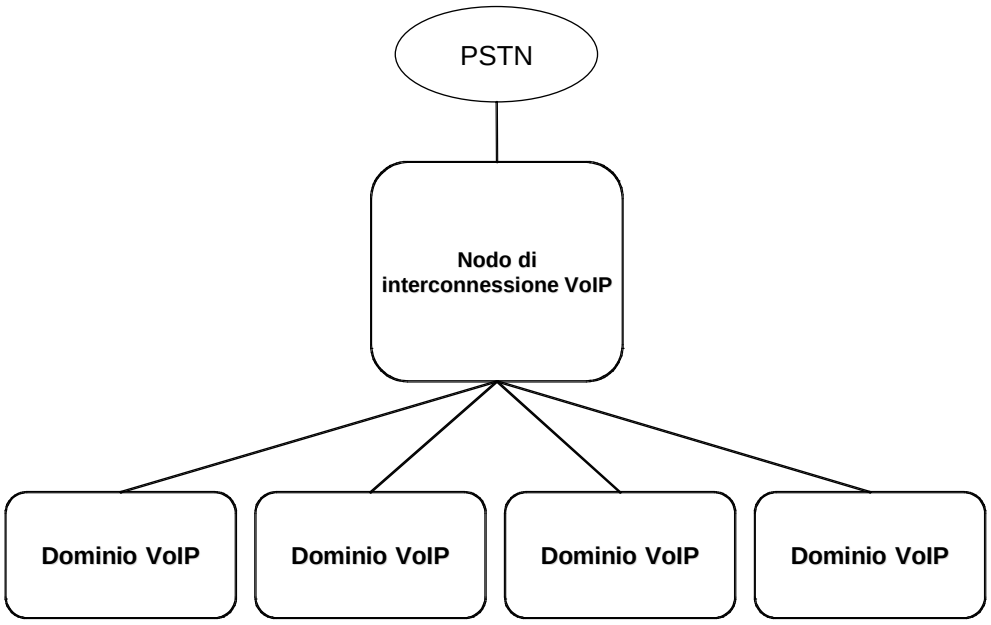

Figura 2 - Architettura di riferimento del servizio telefonia su IP

Un'amministrazione potrà decidere di dotarsi, sulla base di elementi amministrativi della propria organizzazione interna, di uno o più domini VoIP.

Il fornitore assegnatario dovrà realizzare il dominio VoIP per la fornitura del servizio VoIP, includendo i seguenti elementi funzionali:

- postazioni VoIP di tipo Stazioni telefoniche IP e di tipo Stazioni applicative IP;
- Session Control Server (SCS): elemento funzionale sede dell'esecuzione della logica di servizio;

- Business Gateway (BGW): elemento funzionale cui è demandato l'interfacciamento con PBX pre-esistenti e, su richiesta della amministrazione stessa, con la rete PSTN.

Il fornitore assegnatario dovrà altresì dimensionare opportunamente ogni elemento del dominio VoIP in funzione delle richieste di traffico da parte della amministrazione.

In riferimento ad ogni singolo dominio VoIP, la funzione SCS, sede dell'esecuzione della logica del servizio, dovrà essere dispiegata dal fornitore assegnatario secondo una delle due modalità operative di seguito descritte, a seconda della richiesta dell'amministrazione:

- modalità **managed IP-Telephony** (Figura 3): la funzione verrà fisicamente implementata attraverso l'utilizzo di apparati situati in siti della amministrazione, comunque manutenti e monitorati dal fornitore;
- modalità **hosted IP-Telephony** (Figura 4): la funzione verrà fisicamente implementata attraverso l'utilizzo di uno o più apparati situati in uno o più centri del fornitore, in condivisione tra differenti domini VoIP, eventualmente acquisti da differenti amministrazioni, mantenendo di fatto una separazione logica tra i vari domini VoIP.

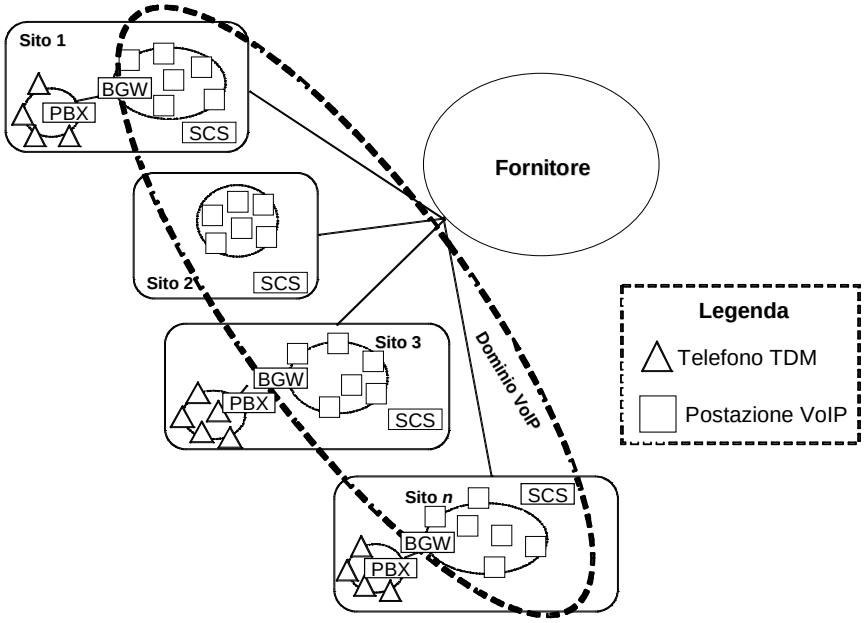

Figura 3 - Architettura di riferimento 'dominio VoIP' – managed

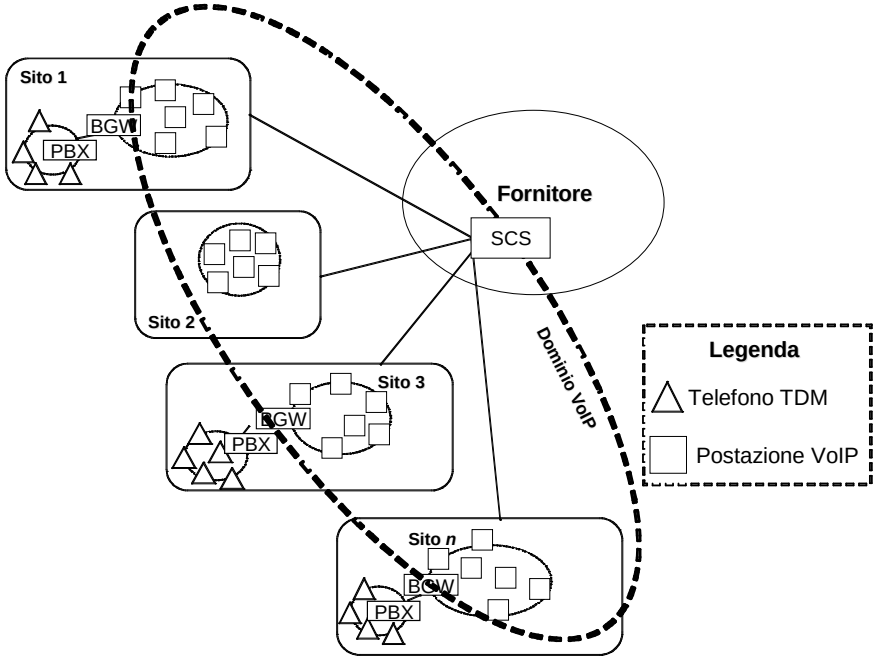

Figura 4 - Architettura di riferimento 'dominio VoIP' – hosted

Le interfacce esterne del dominio VoIP rappresentano i punti di confine della responsabilità amministrativa e gestionale del fornitore assegnatario. Tali interfacce, evidenziate nella Figura 5, sono elencate e caratterizzate nella Tabella 9.

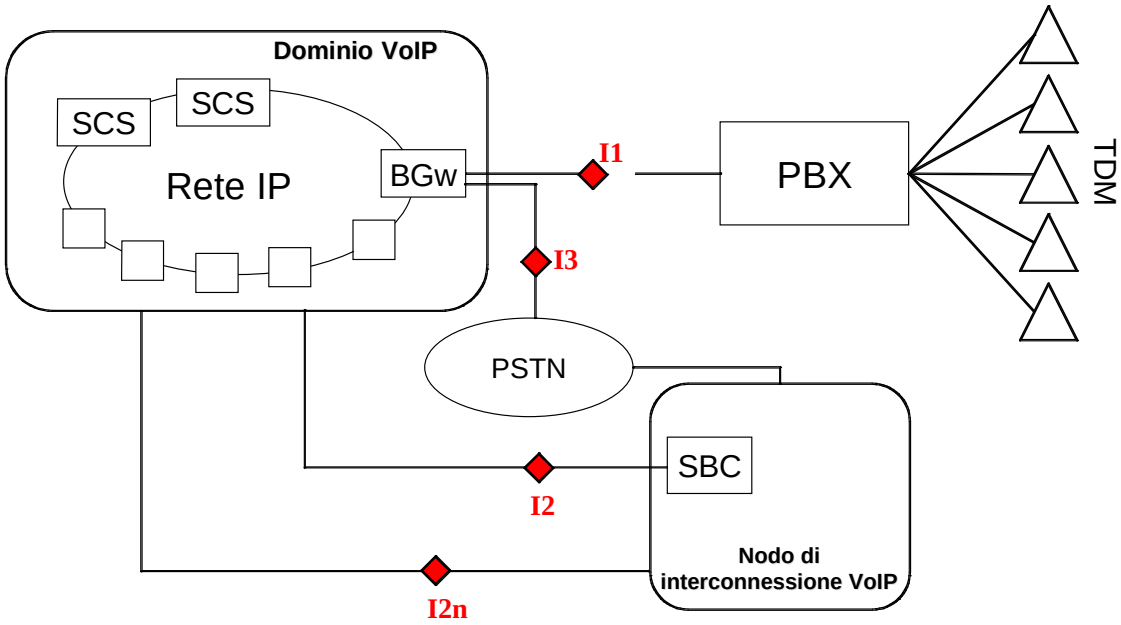

Figura 5 - Interfacce esterne del dominio VoIP

Identificativo interfaccia	Tipo interfaccia	Descrizione
Interfaccia I1	ISDN o Q.SIG	Interfaccia di connessione al PBX pre-esistente. La disponibilità di tale interfaccia sul PBX è a carico della amministrazione. Qualora vi sia un accordo con la società che ha in carico la gestione del PBX e vi sia una compatibilità tecnologica, l'interfaccia I1 può essere collassata internamente al PBX inserendo una scheda VoIP all'interno del PBX.
Interfaccia I2	H.323 o SIP RTP	Interfaccia di connessione al nodo di interconnessione VoIP per lo scambio di chiamate telefoniche (sia segnalazione che informazione vocale). L'accesso a tale servizio verrà effettuato attraverso un punto di connessione logico messo a disposizione dal fornitore del servizio di nodo di interconnessione VoIP su uno dei propri Session Border Controller (SBC). Tale interfaccia dovrà essere implementata, a discrezione del fornitore assegnatario, secondo il protocollo H.323 oppure il protocollo SIP, per quanto riguarda la segnalazione. L'informazione vocale dovrà essere invece trasportata per mezzo del protocollo RTP.

Interfaccia I2n	-	Interfaccia utilizzata per lo scambio delle informazioni di instradamento a livello VoIP tra il fornitore assegnatario ed il nodo di interconnessione VoIP. Per quanto concerne il/i protocollo/i da utilizzare su questa interfaccia, il fornitore dovrà sviluppare la soluzione in accordo alle indicazioni prese da CNIPA sentiti i fornitori assegnatari del presente capitolato e il gestore del nodo di interconnessione VoIP.
Interfaccia I3	ISDN BRI o PRI	Interfaccia di accesso ISDN BRI o PRI alla rete di telefonia pubblica. Il BGW deve essere configurato come TE ISDN con I3 corrispondente al punto di riferimento T dell'architettura ISDN.

Tabella 9: Interfacce esterne del Dominio VoIP

Non essendo il nodo di interconnessione VoIP oggetto della presente gara, le interfacce I2 e I2n dovranno essere rese disponibili contestualmente alla disponibilità del nodo di interconnessione.

Il dimensionamento di tali interfacce (in termini di numero e capacità) dovrà essere effettuato dal fornitore sulla base di ogni singolo progetto, ovvero di ogni dominio VoIP installato, nel rispetto delle esigenze di traffico espresse dalle singole amministrazioni.

Il fornitore dovrà introdurre il dominio VoIP in modo congruente e compatibile con il piano di numerazione pre-esistente. Sulla base delle richieste dell'amministrazione, le postazioni VoIP dovranno:

- riutilizzare numerazioni interne già assegnate in precedenza al dominio tradizionale, oppure
- utilizzare nuove estensioni, oppure
- introdurre un piano di numerazione ex-novo utilizzando una diversa radice.

Il fornitore assegnatario sarà responsabile dell'implementazione all'interno del dominio VoIP di tutte le funzionalità necessarie alla risoluzione di problemi relativi all'attraversamento di elementi di rete su cui è attiva la funzione di Network Address Translation (secondo una qualunque delle sue declinazioni, ad esempio Port Address Translation) per quanto riguarda i servizi inter-dominio e di interfacciamento PSTN centralizzato, ovvero le comunicazioni telefoniche scambiate con il nodo di interconnessione VoIP attraverso l'interfaccia I2. Il fornitore assegnatario sarà altresì responsabile dell'opportuna e congruente gestione di eventuali firewall sotto la sua amministrazione che possano impattare sul servizio di telefonia su IP.

1.3.3 Elementi funzionali dell'architettura

Stazioni telefoniche IP

Il fornitore assegnatario dovrà fornire stazioni telefoniche IP che supportino le seguenti caratteristiche:

- connessione diretta mediante interfaccia Ethernet alla rete IP;

- tele-alimentazione remota attraverso l’interfaccia Ethernet e alimentazione locale a 120/230V;
- supporto dell’assegnazione dinamica dell’indirizzo IP mediante il protocollo DHCP (IETF RFC2131);
- implementazione della funzione di H.323 terminal oppure della funzione di SIP User Agent.

Si richiedono le tipologie di stazioni telefoniche IP caratterizzate dai seguenti requisiti minimi:

- Tipo 1: postazioni di supervisione o utente per la gestione di traffico intenso:
  - monitor con lettura di 2 righe x 40 caratteri
  - controllo del contrasto
  - 5 tasti sensibili al contesto (soft-key)
  - tastiera alfanumerica
  - modalità di ascolto viva voce e amplificata
  - 15 tasti programmabili dall'utente e dall'amministratore del sistema
  - icone LCD di segnalazione associate a ogni tasto
  - rubrica personale con 50 nomi
  - controllo del volume per il ricevitore
  - servizio di guida in linea integrato per le operazioni di programmazione

- Tipo 2: stazioni per assistenti o utenti che gestiscono traffico medio:
  - monitor con lettura di 2 righe x 20 caratteri
  - controllo del contrasto
  - 3 tasti sensibili al contesto (soft-key)
  - tastiera alfanumerica
  - modalità di ascolto viva voce e amplificata
  - 15 tasti programmabili dall'utente e dall'amministratore del sistema
  - icone LCD di segnalazione associate a ogni tasto
  - rubrica personale con 15 nomi
  - controllo del volume per il ricevitore
  - servizio di guida in linea integrato per le operazioni di programmazione

- Tipo 3: stazioni per utenti con traffico normale:
  - monitor con lettura di 1 riga x 20 caratteri
  - modalità di ascolto viva voce e amplificata
  - 4 tasti programmabili dall'utente e dall'amministratore del sistema
  - segnali associati a ogni tasto con simboli di tipo icona
  - rubrica personale con 12 numeri
  - regolazione del volume del ricevitore
  - servizio di guida in linea integrato per le operazioni di programmazione

Le stazioni telefoniche IP dovranno garantire un utilizzo semplice senza differenze nelle interfacce utente e nei servizi. I terminali, inclusi quelli di livello inferiore, devono includere tasti che possono essere programmati direttamente dall'utente. Tali tasti dovranno permettere la concatenazione di diverse funzioni (ad esempio codice di richiamata + numero esterno e così via).

Le stazioni telefoniche IP dovranno supportare i servizi elencati nel paragrafo 1.3.4 .

Stazioni applicative IP

Il fornitore assegnatario dovrà proporre una stazione applicativa IP, ovvero un'applicazione software eseguibile su Personal Computer, completa di funzionalità di connessione e telefonia IP integrate, in grado di supportare qualsiasi applicazione aziendale per il Web compatibile con lo standard XML.

Le stazioni applicative IP dovranno implementare la funzione di H.323 terminal oppure la funzione di SIP User Agent.

Le Stazioni applicative dovranno essere installabili ed eseguibili sui seguenti sistemi operativi: Microsoft Windows 2000, Microsoft Windows XP, Apple MacOS X (a partire dalla versione 10.2).

La fornitura delle stazioni applicative IP non comprende l'hardware su cui esse verranno utilizzate, né eventuali sistemi di interfacciamento con l'utente quali microfono e cuffie.

Le stazioni applicative IP dovranno supportare i servizi elencati nel paragrafo 1.3.4 .

Session Control Server

Il Session Control Server è l'entità che gestisce la segnalazione per il controllo delle fasi di una chiamata, o più in generale di una sessione multimediale. È la sede della logica di servizio per la realizzazione di tutti i servizi intra-dominio (e, se richiesto dall'amministrazione, di interfacciamento PSTN locale), e collabora con elementi esterni al dominio VoIP per i servizi inter-dominio (e, se richiesto dall'amministrazione, di interfacciamento PSTN centralizzato).

Il Session Control Server dovrà includere le seguenti funzioni:

- Incoming Call Gateway (ICGW): per quanto riguarda la segnalazione, rappresenta il punto di ingresso al dominio VoIP e si prende carico del corretto instradamento delle chiamate all'interno del dominio;
- Call Control Function (CCF): è responsabile dell'attivazione e del rilascio delle chiamate e della gestione degli stati della chiamata e degli eventi di cambiamento dello stato stesso. Determina la necessità della funzione di transcodifica per le chiamate/sessioni. Controlla inoltre eventuali MultiConference Unit (MCU) per la realizzazione dei servizi multi-party. Gestisce infine la registrazione delle postazioni VoIP. Opzionalmente la funzione CCF è anche responsabile di interfacciarsi con Application Server esterni per la realizzazione/controllo di servizi a valore aggiunto;
- Serving Profile Database: funzione di gestione e controllo dei profili delle utenze VoIP, includendo anche le informazioni relative all'autorizzazione, all'utilizzo delle differenti tipologie di servizio intra-dominio, inter-dominio e interfacciamento PSTN;
- Address Handling: gestisce l'analisi, la traduzione, la modifica se necessario, e la risoluzione degli indirizzi da identificativo alfanumerico a indirizzo IP;
- Signalling Interworking: opzionalmente, il SCS può includere una funzione di gestione della segnalazione Q.931 per l'interfacciamento con la rete telefonica pubblica opportunamente adattata allo stack protocollare IP. Sarà compito del BGW eseguire l'adattamento protocollare tra stack ISDN e IP.

Business Gateway

La funzione Business Gateway fornisce il canale dei media tra il dominio VoIP ed uno o più PBX pre-esistenti. Inoltre, se richiesta dalla amministrazione, il BGW dovrà essere in grado di essere

connesso alle reti telefoniche pubbliche PSTN/PLMN utilizzando accessi ISDN PRI oppure ISDN BRI.

Il BGW dovrà inoltre includere le funzionalità necessarie a modificare i canali media:

- encoding;
- cancellazione d'eco;
- pacchettizzazione;
- transcodifica;
- sincronizzazione dei flussi RTP corrispondenti ai differenti flussi media di una sessione multimediale.

Sulle interfacce verso il PBX pre-esistente e verso la rete telefonica pubblica il BGW dovrà essere in grado di codificare e decodificare canali PCM in codifica G.711, ed applicare la transcodifica necessaria secondo la negoziazione del codec avvenuta nel dominio VoIP. Verso il dominio IP, il BGW è inoltre responsabile della generazione e della terminazione dei flussi RTP.

Per quanto concerne la segnalazione, il BGW dovrà essere in grado di gestire la segnalazione Q.931 utilizzata dagli accessi ISDN lato PSTN e convertirla nel protocollo di segnalazione utilizzato all'interno del dominio VoIP. Alternativamente il BGW potrà inoltrare la segnalazione Q.931 sino al Session Control Server, applicando un'opportuna funzione di adattamento di stack protocollare tra ISDN e IP.

Il BGW dovrà essere in grado di connettersi a PBX tradizionali (basati su tecnologia TDM), utilizzando interfacce ISDN oppure Q.SIG.

1.3.4 Funzionalità di fonia

Servizi intra-dominio

All'interno del dominio VoIP il fornitore assegnatario dovrà erogare servizi di fonia intra-dominio (cfr. Tabella 10).

Servizi intra-dominio
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
Funzioni FAX

Tabella 10: Servizi intra-dominio

In aggiunta ai servizi sopra-elencati, il fornitore è tenuto ad offrire il servizio di segreteria telefonica, qualora richiesto dall'amministrazione.

Servizi inter-dominio

Il fornitore assegnatario dovrà supportare i servizi inter-dominio elencati in Tabella 11, qualora gli end-point coinvolti dalla chiamata, siano essi postazioni VoIP oppure Business Gateway, appartengano a domini VoIP distinti:

Servizi di fonia inter-dominio
Chiamata base
Presentazione dell'indirizzo/alias del chiamante
Trasporto dei toni DTMF
Funzioni FAX

Tabella 11: Servizi inter-dominio

In aggiunta ai servizi sopra-elencati, il fornitore assegnatario è tenuto ad offrire il servizio di segreteria telefonica, qualora richiesto dall'amministrazione.

Servizi di interfacciamento con PSTN

La soluzione proposta dal fornitore assegnatario dovrà supportare i servizi di interfacciamento PSTN, elencati in Tabella 12, verso/da rete PSTN.

Servizi di interfacciamento con PSTN
Chiamata base
Presentazione dell'indirizzo/alias del chiamante

Trasporto dei toni DTMF
Funzioni FAX

Tabella 12: Servizi di interfacciamento PSTN

In aggiunta ai servizi sopra-elencati, il fornitore assegnatario sarà tenuto ad offrire il servizio di segreteria telefonica, qualora richiesto dall'amministrazione.

1.3.5 Instradamento delle chiamate

Servizi intra-dominio

All'interno del dominio VoIP sarà responsabilità del fornitore assegnatario la gestione dell'instradamento completo di tutti i servizi intra-dominio precedentemente elencati (cfr. Figura 6 [a]).

Il fornitore assegnatario dovrà inoltre prendersi carico, fino al punto di interconnessione BGW-PBX (cfr. Figura 5, [interfaccia I1]), dell'instradamento di tutte le chiamate (cfr. Figura 6 [b]) telefoniche che coinvolgano almeno una postazione VoIP (in qualità di chiamante o chiamato).

Le chiamate tra due telefoni tradizionali connessi al PBX TDM non dovranno essere gestite dal fornitore, essendo interamente al di fuori del dominio VoIP.

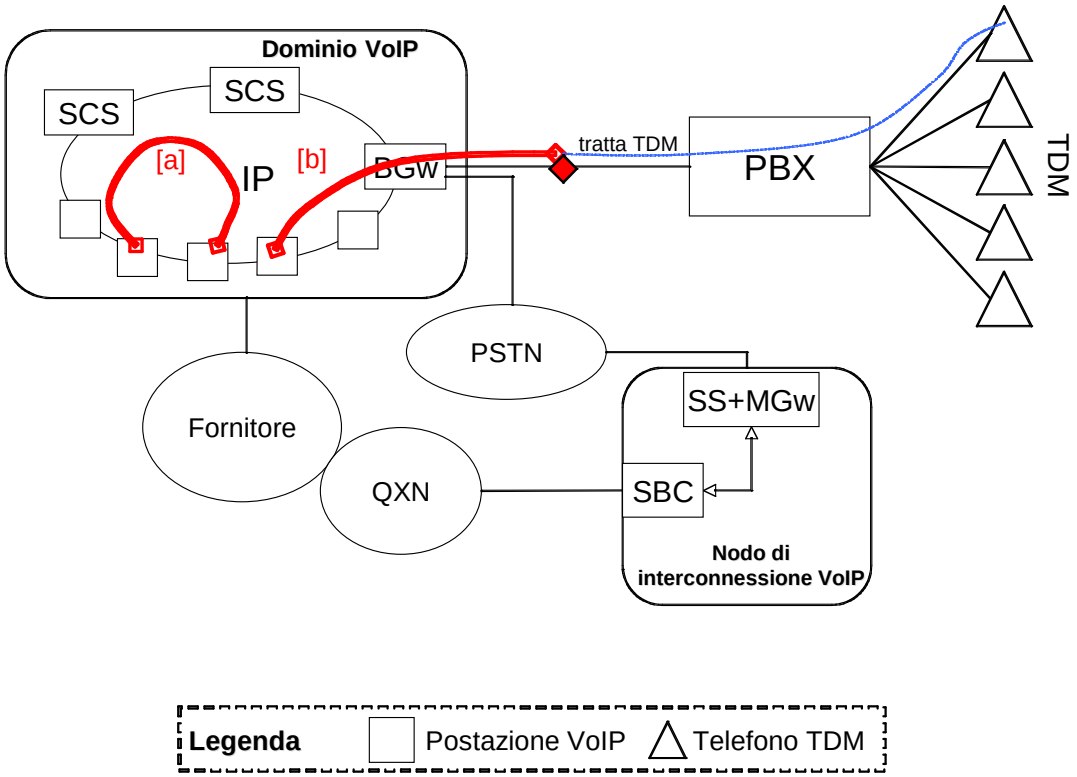

Figura 6 - Instradamento servizi intra-dominio

Servizi inter-dominio

I servizi di fonia inter-dominio coinvolgono due domini VoIP distinti cui rispettivamente appartengono l'utente chiamante e l'utente chiamato.

Tutte le chiamate originate da postazioni VoIP appartenenti ad un qualunque dominio VoIP e destinate a postazioni VoIP appartenenti ad un qualunque altro dominio VoIP dovranno transitare attraverso il nodo di interconnessione VoIP indipendentemente dai fornitori che li gestiscono, come in Figura 7.

A tal fine, il fornitore assegnatario dovrà comunicare al nodo di interconnessione VoIP, attraverso l'interfaccia I2n, tutti gli archi di numerazione relativi alle postazioni VoIP da lui gestite/operate.

Non è pertanto ammessa la possibilità di chiamate tra domini VoIP distinti non transitanti attraverso il nodo di interconnessione VoIP.

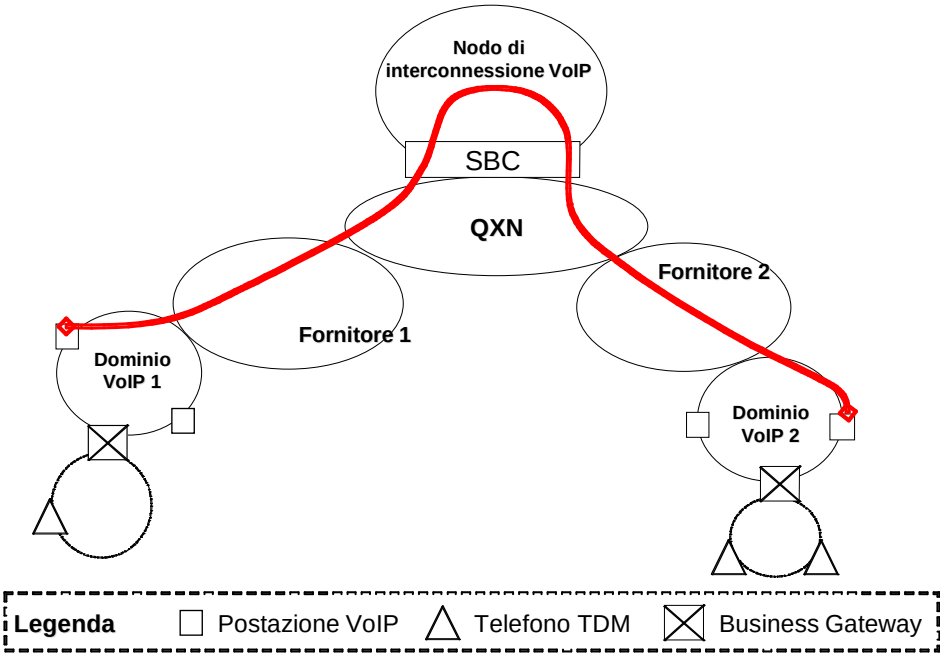

Figura 7 - Instradamento servizi inter-dominio (1/2)

Inoltre:

- il fornitore assegnatario, se richiesto dall'amministrazione, è tenuto a comunicare al nodo di interconnessione VoIP, utilizzando l'interfaccia I2n, tutti gli archi di numerazione associati a telefoni tradizionali TDM raggiungibili attraverso Business Gateway gestiti dal fornitore, verso i quali il fornitore assegnatario stesso dovrà garantire la raggiungibilità per tutte le chiamate in ingresso ricevute dal nodo di interconnessione VoIP attraverso l'interfaccia I2 (cfr. Figura 8 [a]).
- il fornitore assegnatario è tenuto ad instradare verso il nodo di interconnessione VoIP (cfr. Figura 8 [b]), utilizzando l'interfaccia I2, tutte le chiamate generate da una postazione VoIP oppure da un Business Gateway sotto la sua gestione, dirette verso tutti gli archi di numerazione (non facenti parte del dominio di origine) che verranno comunicati dal nodo di interconnessione al fornitore assegnatario stesso per mezzo dell'interfaccia I2n.

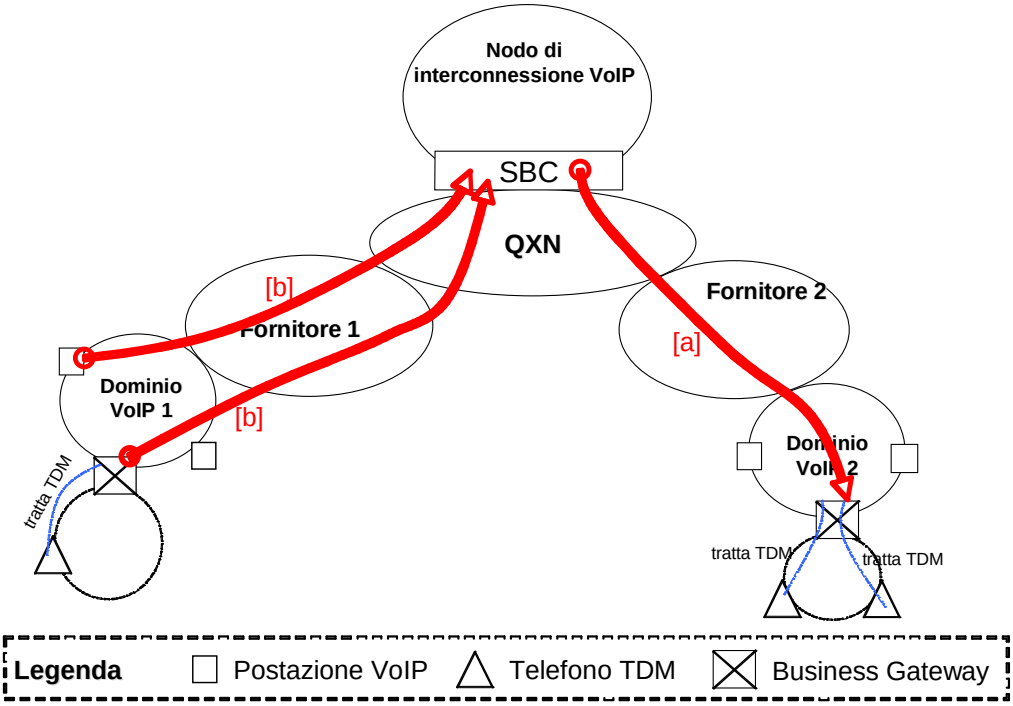

Figura 8 - Instradamento servizi inter-dominio (2/2)

In tutti i casi descritti, i limiti di responsabilità del fornitore assegnatario saranno le interfacce esterne del dominio VoIP descritte nel paragrafo 1.3.2 (cfr. Figura 5).

Servizi di interfacciamento PSTN

L'amministrazione che acquista il servizio di IP-Telephony potrà scegliere tra due differenti opzioni per l'interconnessione del dominio VoIP alla rete telefonica pubblica (PSTN):

- servizio di interfacciamento PSTN locale;
- servizio di interfacciamento PSTN centralizzato (offerto e gestito dal nodo di interconnessione VoIP).

Qualora l'amministrazione decida di avvalersi di un servizio di interfacciamento PSTN locale, il fornitore dovrà equipaggiare il Business Gateway inserendo interfacce ISDN BRI o PRI in numero tale da soddisfare i requisiti tecnologici e di traffico espressi dall'amministrazione.

All'interno del dominio VoIP, origine o terminazione dei servizi di interfacciamento PSTN locale potrà essere sia una postazione VoIP (cfr. Figura 9 [a]) sia un telefono tradizionale raggiunto attraverso un qualunque Business Gateway appartenente al dominio VoIP (cfr. Figura 9 [b]).

Qualora l'amministrazione si appoggi al servizio di interfacciamento PSTN locale offerto dal fornitore, quest'ultimo sarà tenuto alla gestione completa del piano di numerazione di tutte le utenze raggiungibili attraverso il dominio VoIP per quanto concerne le chiamate entranti da PSTN che verranno convogliate al BGW come previsto dall'architettura (cfr. paragrafi 1.3.2 e 1.3.3).

Il servizio di interfacciamento PSTN locale non comprende il servizio di commutazione del traffico su rete telefonica pubblica ed il relativo rilegamento trasmissivo, dei quali l'amministrazione dovrà approvvigionarsi in modo autonomo.

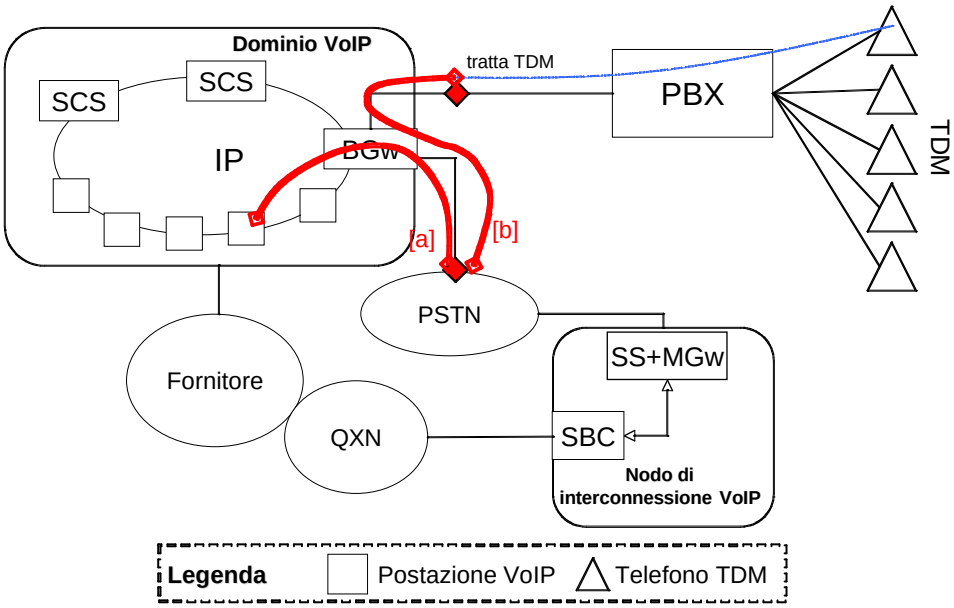

Figura 9 - Instradamento dei servizi di interfacciamento PSTN locale

In alternativa l'amministrazione potrà avvalersi del servizio di interfacciamento PSTN centralizzato offerto dal nodo di interconnessione VoIP. In tal caso il fornitore sarà tenuto ad inoltrare tutti i servizi di fonia interfacciamento PSTN al nodo di interconnessione VoIP (cfr. Figura 10 [a] e [b]) attraverso l'interfaccia I2.

Qualora l'amministrazione decida di attivare il servizio di interfacciamento PSTN centralizzato, il nodo di interconnessione VoIP si prenderà carico, nei confronti della PSTN, dell'intero piano di numerazione di tutte le utenze raggiungibili attraverso il dominio VoIP, siano esse postazioni VoIP che telefoni TDM raggiungibili attraverso Business Gateway. Il fornitore dovrà quindi terminare correttamente tutte le chiamate ricevute in ingresso dal nodo di interconnessione VoIP attraverso l'interfaccia I2.

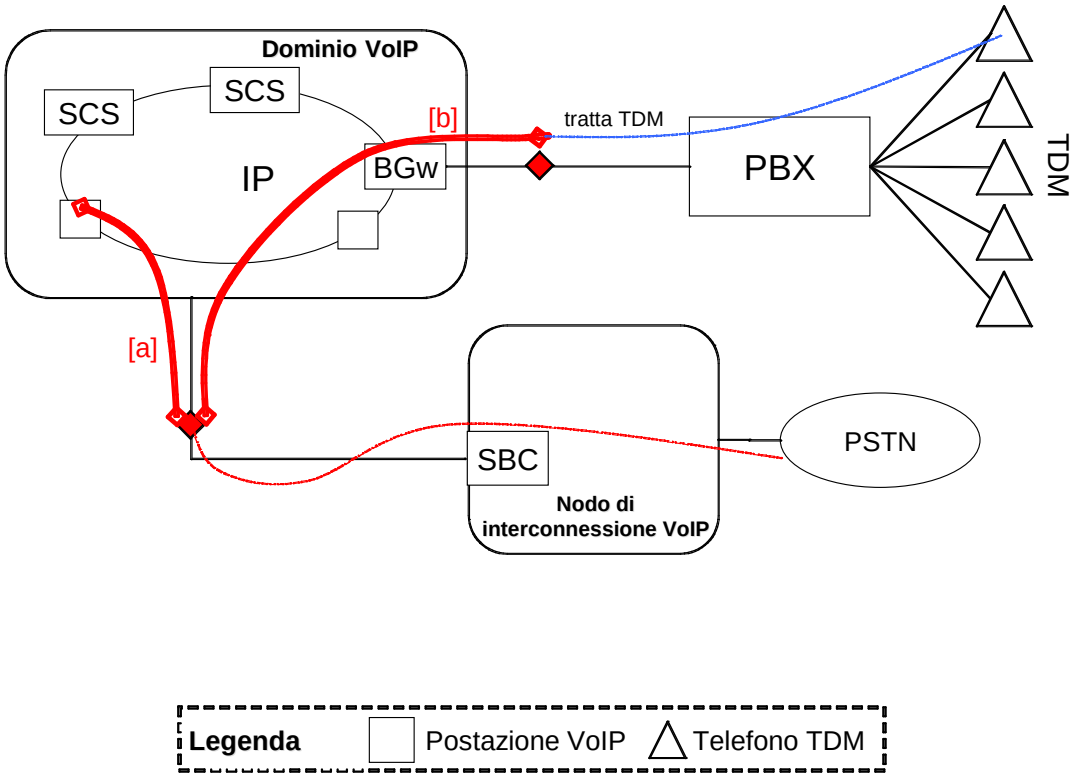

Figura 10 - Instradamento dei servizi di interfacciamento PSTN centralizzato.

1.3.6 Affidabilità

Qualora si perda la connettività verso il nodo di interconnessione VoIP, il fornitore dovrà garantire al dominio VoIP i seguenti servizi:

- sopravvivenza funzionale dei servizi di centralino locali e, se richiesto dall'amministrazione, del servizio di interfacciamento PSTN locale;
- accessibilità ai servizi di emergenza.

1.3.7 Autenticazione ed autorizzazione

All'interno del dominio VoIP il fornitore dovrà supportare servizi di autenticazione ed autorizzazione nei confronti degli utenti che utilizzano postazioni VoIP. Tali servizi devono essere offerti mediante comunicazioni logiche IP sicure.

Per quanto riguarda l'autenticazione, il fornitore dovrà supportare l'autenticazione dell'utente.

Per quanto riguarda l'autorizzazione il fornitore dovrà essere in grado di implementare servizi di white list e black list sulla base della coppia <numero dei chiamante, numero del chiamato>.

L'autenticazione dell'utente dovrà essere realizzata mediante comunicazioni sicure, ad esempio utilizzando:

- ITU-T H.235v2: comunicazioni sicure per il protocollo H.323;
- IETF RFC 2617: comunicazioni sicure per il protocollo SIP.

1.3.8 Standard di riferimento

La soluzione proposta dal fornitore assegnatario dovrà essere conforme agli standard di riferimento di seguito elencati per le differenti famiglie di protocolli.

Il fornitore dovrà specificare se la soluzione proposta è conforme ad altri protocolli oppure ad ulteriori standard rispetto agli stessi protocolli elencati.

SIP	IETF RFC 3261	SIP: Session Initiation Protocol
	IETF RFC 2327	Session Description Protocol (SDP)
	IETF RFC 3966	The tel URI for Telephone Numbers
	IETF RFC 2617	HTTP Authentication: Basic and Digest Access Authentication

H.323	ITU-T H.323 v4	H.323 - Packet-based multimedia communications systems
	ITU-T H.225.0 v4	H.323 - call control protocol
	ITU-T H.245v7	H.323 – media control protocol
	ITU-T H.235v2	H.323 - security

RTP/RTCP	IETF RFC 3550	RTP: Transport Protocol for Real-Time Applications
	IETF RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

Codifica dell'informazione vocale	ITU-TG.711	Pulse code modulation (PCM) of voice frequencies
	ITU-T G.723.1	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s
	ITU-T G.729	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP)

MGCP	IETF RFC 3435	Media Gateway Control Protocol (MGCP) Version 1.0
	IETF RFC 3660	Basic Media Gateway Control Protocol Packages
	IETF RFC 3661	MGCP Return Code Usage

H.248	ITU-T H.248v1	Media Gateway control protocol v.1
	ITU-T H.248v2	Media Gateway control protocol v.2
	IETF RFC 3525	Gateway Control Protocol Version 1

SIGTRAN	IETF RFC 2719	Architectural Framework for Signaling Transport
	IETF RFC 2960	Stream Control Transmission Protocol
	IETF RFC 3332	SS7 MTP3-User Adaptation Layer (M3UA)
	IETF RFC 3057	ISDN Q.921-User Adaptation Layer

ENUM	IETF RFC 3761	The E.164 to URI DDDS Application (ENUM)
	IETF RFC 3482	Number Portability in the Global Switched Telephone Network (GSTN): An Overview

RADIUS	IETF RFC 2865	Remote Authentication Dial In User Service (RADIUS)
	IETF RFC 2866	RADIUS Accounting
	IETF RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support

DHCP	RFC 2131	Dynamic Host Configuration Protocol

ISDN	ETSI ETS 300 012	ETSI ISDN Basic Rate
	ETSI ETS 300 011, ETS 300 402	ETSI ISDN Primary Rate
	ETSI ITU Q.931	Standard DSS1

Norme interconnessione	L'interconnessione con la PSTN richiede il supporto della Regola Tecnica N.763 del Ministero delle Poste e delle Telecomunicazioni.
	L'interconnessione a PSTN può essere ottenuta anche in accordo alla specifica Regola Tecnica N. 748, capitoli 1-9 (ISUP-S).
	La soluzione proposto deve essere conforme allo standard ITU-T Q.767 (ISUP) e ad altri standard normalmente richiesti per l'interconnessione a carrier internazionali.
	L'interworking con operatori mobili richiede la conformità con le specifiche ETSI ISUP 300 303 e ETSI ISUP 300 356.

Tabella 13: Protocolli VoIP

1.4 Servizi di interoperabilità di base

Il fornitore assegnatario dovrà erogare i seguenti servizi di interoperabilità di base, ovvero i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici:

- **Posta elettronica**: consente l'interconnessione tra diversi domini a livello applicativo per lo scambio di messaggi di Posta elettronica.
- **Trasporto di protocolli proprietari**: consente il trasporto del protocollo SNA su IP.
- **Servizi di Data Center**.

1.4.1 Posta elettronica

Il servizio erogato dal fornitore assegnatario dovrà consentire l'interconnessione tra diversi domini a livello applicativo per lo scambio di messaggi di posta elettronica. I messaggi dovranno poter contenere dati con qualsiasi formato, inclusi i formati EDI.

Il servizio dovrà 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.

Il fornitore assegnatario dovrà prevedere, per l'espletamento delle funzionalità di posta elettronica, la gestione di un mailer per i messaggi scambiati da e verso gli ambiti delle altre amministrazioni e l'ambito Internet.

Il fornitore dovrà erogare un servizio di posta elettronica caratterizzato dalle seguenti funzionalità:

- controllo antivirus sui messaggi scambiati attivabile e disattivabile su richiesta;
- assegnazione e gestione degli account di posta nello spazio di naming concordato con le amministrazioni;
- accesso alle caselle attraverso i protocolli SMTP, POPv3, IMAPv4, POPS e IMAPS;
- accesso alle caselle attraverso protocollo HTTP, HTTPS ed interfaccia Web.

Il fornitore assegnatario dovrà assicurare la continuità del servizio di posta elettronica prevedendo adeguati meccanismi di "backup a caldo" che evitino perdite di informazioni scambiate.

Lo scambio bidirezionale di posta elettronica fra due domini di amministrazioni dovrà essere assicurato nel rispetto dei requisiti di sicurezza riportati nel paragrafo 1.5.2 .

Il fornitore assegnatario dovrà 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 solo vincolo di prevedere almeno 10 MByte a casella per la memorizzazione dei messaggi e di altri dati inseriti dall'utente.

Il fornitore assegnatario dovrà 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.

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.

Il fornitore assegnatario dovrà 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).

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.

1.4.2 Trasporto di protocolli proprietari

Il fornitore assegnatario dovrà erogare, su richiesta dell'amministrazione, un servizo di trasporto del protocollo SNA su IP al fine di garantire:

- il funzionamento di dispositivi collegati all'host tramite protocollo SDLC, QLLC o LLC;
- l'accesso alle applicazioni "legacy" su host da parte dei PC in LAN.

Il fornitore assegnatario dovrà garantire un servizio che supporti il collegamento con l'host di Logical Unit di tipo 0, 1, 2 e 3 tramite la TdR.

Il fornitore assegnatario dovrà prevedere sia una soluzione di trasporto SNA su IP di tipo "bridged" (es. DLSw v1 e v2, RFC1795 e RFC2166), sia di tipo "routed" (es. APPN/HPR su IP, RFC2353). Per il DLC LLC il punto di accesso al servizio di trasporto SNA sarà l'interfaccia PAS della TdR. Per il DLC SDLC e QLLC il punto di accesso al servizio di trasporto SNA sarà un'ulteriore interfaccia del router, di seguito definita I_SNA_CLIENT. A seconda del numero di apparati da connettere all'interfaccia I_SNA_CLIENT, quest'ultima dovrà essere costituita di un idoneo numero di interfacce seriali in configurazione punto-punto o punto-multipunto (SDLC).

1.4.3 Servizi di Data Center

Il fornitore assegnatario dovrà erogare i seguenti servizi, definiti di Data Center:

- **hosting**;
- **housing**.

L'amminsitrazione potrà richiedere al fornitore il collegamento degli apparati ospitati tramite il servizio di Housing o utilizzati per il servizio di hosting ad una LAN locale on interfacce ethernet/fast ethernet o Gigabit Ethernet. Il fornitore dovrà erogare servizi di trasporto da e per i Server localizzati nei Data Center all'SPC con le stesse caratteristiche dei servizi alway-on e con le stesse modalità di pricing previste per le sole componenti i trasferimento (CdT).

Il fornitore assegnatario dovrà garantire che i locali che ospiteranno i sistemi per l'erogazione dei servizi di Data Center posseggano i seguenti requisiti:

- **Impianto di condizionamento**, che garantisca i seguenti requisiti ambientali:

    - ricambi d’aria: 0,5 volumi/ora;
    - temperatura: 25±1 °C;
    - umidità relativa: controllata (35-65%).
- **Gruppi di continuità**: la continuità del sistema dovrà essere garantita da un set di batterie con autonomia tale da garantire il funzionamento complessivo nel tempo necessario all’attivazione del sistema di emergenza. Tale sistema dovrà avere un’autonomia minima di 48 ore a pieno carico.
- **Rilevazione fumi ed impianto antincendio**: il fornitore assegnatario dovrà dotare di rilevatori antifumo e sistemi antincendio tutti gli ambienti in cui sono alloggiati i server.
- **Sistemi anti-allagamento**: il fornitore assegnatario dovrà prevedere sonde di rilevazione per la presenza di liquidi sotto il pavimento flottante e dotare gli ambienti di sistemi di convogliamento e scarico dei liquidi verso l’esterno.
- **Sistemi anti-intrusione**: il fornitore assegnatario dovrà dotare tutti gli ambienti in cui sono alloggiati i server di sistemi anti-intrusione integrati con un impianto di video sorveglianza. Il fornitore assegnatario dovrà posizionare videocamere a circuito chiuso al fine di consentire il monitoraggio del perimetro dell’edificio, degli ingressi, delle porte e di eventuali altre zone critiche e/o di accesso.
- **Controllo degli accessi fisici**: il fornitore assegnatario dovrà garantire un servizio di sorveglianza 24 ore su 24 che provveda all’identificazione del personale che accede ai locali, all’esecuzione di procedure di registrazione degli accessi. I locali dovranno essere dotati di dispositivi di accesso tramite badge.
- **Disponibilità di rack** con le seguenti caratteristiche:
    - misure:
        - 19” e 800x1000x2280 mm oppure 800x800x2280 mm (LxPxH);
        - 22” e 800x1000x2280 mm (LxPxH);
    - sistema doppio di alimentazione e di distribuzione dell’energia elettrica e interruttori magnetotermici differenziali di idonee caratteristiche;
    - armadio in lamiera di acciaio con spazio libero ai lati dei montanti, in modo da permettere la canalizzazione di cavi e fibre, rispettando il raggio minimo di curvatura ammissibile;
    - porta frontale in materiale trasparente di dimensioni tali da consentire la visibilità dell’interno e dotata di maniglia con serratura di sicurezza a chiave;
    - pannelli laterali asportabili.

Il fornitore assegnatario dovrà garantire il rilevamento 24 ore su 24 di eventuali tentativi di intrusione sui sistemi ospitati e provvedere alle seguenti attività:

- esecuzione di un’applicazione real-time per la rilevazione delle intrusioni e rilevamento 24x7 di alert system per azioni immediate contro le intrusioni;
- esecuzione periodica di attività di verifica di solidità password, configurazione del sistema operativo ed integrità dei file di sistema;
- registrazione dei tentativi di modifica dei componenti critici del sistema operativo;
- prevenzione di accessi non autorizzati (in particolare ai servizi TCP e UDP);

- registrazione di tutti i tentativi di login (in particolare Telnet, FTP, SSH, UDP);
- installazione antivirus;
- traccia e notifica all'amministrazione di eventuali tentativi di violazione.

Hosting

Il fornitore assegnatario dovrà erogare un servizio di hosting, consistente nel fornire all'amministrazione l'hardware ed il software necessari per gestire il server Web che verrà alimentato con pagine prodotte dall'amministrazione stessa.

Il fornitore assegnatario dovrà effettuare le attività di seguito indicate:

- Configurazione iniziale dei server: hardware, software di base e web server.
- User administration (a livello di sistema operativo, non applicativo e/o database):
    - creazione utenze Telnet/FTP e relative password per consentire l'accesso all'amministrazione;
    - mantenimento del controllo degli accessi e fornitura delle autorizzazioni per accessi individuali (max 10 utenti) e di gruppo (max 10 gruppi di sistema);
    - definizione e gestione degli script di login/logon.
- Amministrazione del Sistema Operativo e del Web Server:
    - gestione File System;
    - gestione processi di base del Sistema Operativo e del Web Server;
    - verifica della disponibilità dell'indirizzo IP ad intervalli di tempo predefiniti;
    - verifica della disponibilità di un Http server ad intervalli di tempo predefiniti;
    - verifica e gestione log di sistema operativo;
    - verifica degli eventi di sicurezza registrati (login errati, tentativi di "defacement", cancellazione/modifica di file non autorizzati, attacchi DOS);
    - implementazione e gestione di un sistema Host Intrusion Detection;
    - implementazione e gestione di un sistema Antivirus;
    - applicazione patch correttive nel caso di malfunzionamenti.
- Monitoraggio degli indicatori di performance dei server (memoria, occupazione spazio disco, utilizzo del paging, connessioni simultanee).
- Fault management.
- Sincronizzazione con Time Server situato presso il NOC-QXN mediante client NTP installato su Web Server che provvede all'allineamento del tempo ufficiale di rete (cfr. paragrafo 6.3.3).
- Manutenzione hardware del server per il ripristino delle funzionalità originarie nonché riparazione o sostituzione di parti o componenti difettose o guaste.

Il fornitore assegnatario dovrà garantire il back-up dei dati memorizzati sul server fino a un massimo di 100 Gbyte. Il back-up, che potrà riguardare l'intero hard-disk o un insieme limitati di directory che saranno concordate con l'amministrazione, dovrà essere effettuato con:

- metodologia incrementale;
- frequenza giornaliera con mantenimento delle ultime 7 versioni di back-up;
- frequenza settimanale con mantenimento delle ultime 2 versioni di back-up;
- operazioni di restore per fallimenti causati da errori hardware o di software di base;

- operazioni di restore su richiesta dell'amministrazione.

Il fornitore assegnatario dovrà indicare eventuali requisiti tecnologici a carico dell'amministrazione per l'erogazione del servizio.

Housing

Il fornitore assegnatario dovrà erogare un servizio di housing, consistente nell'alloggiamento di un server di proprietà dell'amministrazione all'interno di rack standard condivisi e protetti da chiave.

Il fornitore assegnatario dovrà garantire al personale dell'amministrazione la possibilità di accedere (per lo svolgimento di attività di installazione e collaudo) ai locali secondo l'orario Lunedì-Venerdì 8:00-20:00.

Il fornitore assegnatario dovrà garantire all'amministrazione la possibilità di richiedere lo spegnimento e la riaccensione del server di sua proprietà.

Il fornitore assegnatario dovrà garantire all'amministrazione la possibilità di monitorare le prestazioni delle risorse hardware (RAM, CPU, spazio disco, risorse di rete) e la raggiungibilità del server a livello IP. Tale servizio dovrà essere offerto tramite la pubblicazione su un sito web (accessibile tramite una coppia user-name e password) di report con cadenza settimanale e mensile.

1.5 Manutenzione e assistenza dei servizi di connettività

Nell'ambito dei servizi di connettività il fornitore assegnatario dovrà erogare anche i relativi servizi di manutenzione e assistenza, i quali comprenderanno tutte le attività di gestione dei sistemi e della rete finalizzate a controllare ed intervenire a fronte di anomalie su tutte le componenti dei servizi offerti.

I servizi di manutenzione e assistenza riguarderanno le seguenti attività:

- installazione, attivazione, cessazione e variazione dei servizi e delle relative componenti;
- supervisione della rete e gestione degli apparati;
- mantenimento delle misure di sicurezza minime sulle infrastrutture utilizzate per i servizi di connettività;
- supporto tecnico alla gestione dei malfunzionamenti;
- gestione centralizzata delle configurazioni e distribuzione del software di rete;
- analisi delle prestazioni del servizio;
- rendicontazione;
- supporto alle amministrazioni nell'utilizzo dei servizi oggetto di gara (formazione).

Per l'espletamento di tali servizi il fornitore assegnatario dovrà dotarsi di un **Centro di Gestione di rete** (di seguito indicato con l'acronimo **NOC, Network Operating Center**), integrato con le strutture di supporto utenti del proprio Call Center, in modo da assicurare, nel complesso, i livelli di servizio contrattualizzati (cfr. allegati 2c e 3a).

Il fornitore aggiudicatario dovrà garantire uguali modalità di erogazione dei servizi di manutenzione ed assistenza per l'offerta OPA e per l'offerta OPO.

1.5.1 Network Operating Center (NOC)

Il fornitore assegnatario, limitatamente alla propria infrastruttura di rete, dovrà disporre di un sistema, non necessariamente dedicato ai servizi SPC, basato su architetture e tecnologie standard di tipo SNMP, dedicato alla gestione delle risorse utilizzate per erogare i servizi SPC. Attraverso tale sistema il fornitore assegnatario dovrà 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;
- fornire reportistica almeno per tutti i livelli di servizio definiti, per tutti i servizi contrattualizzati.

Il sistema del fornitore assegnatario dovrà includere una Base Dati contenente informazioni su:

- configurazione delle reti di trasporto in esercizio;
- misurazioni dei livelli di servizio che includono almeno i dati oggetto di tutti i report periodici previsti;
- log dei trouble ticket gestiti dal call center (cfr. paragrafo 1.5.3);
- classificazione dei guasti a seconda dei livelli di servizio contrattualizzati;
- dati di riscontro della qualità.

La Base Dati dovrà essere interamente accessibile in lettura da parte dell'amministrazione mediante Web Browser. Il fornitore assegnatario dovrà a tal fine fornire le credenziali di accesso (username e password secondo le policy definite per il SPC) per la consultazione della Base Dati e per l'esportazione dei dati. In particolare dovranno essere assicurate alle singole amministrazioni le seguenti funzionalità:

- consultazione diretta della Base Dati relativa alla risorse di rete di propria competenza tramite interfaccia grafica che consenta la generazione guidata di report, grafici, e query complesse;
- funzionalità di esportazione dei dati, secondo formati standard, contenuti nella porzione di Base Dati relativa alla risorse di rete di propria competenza.

Il fornitore assegnatario dovrà inoltre fornire alle amministrazioni, dietro richiesta, stazioni di supervisione della rete da installare presso sedi dell'amministrazione. Le stazioni di supervisione dovranno avere visibilità limitata ai soli servizi di trasporto utilizzati dalla singola amministrazione. Le stazioni di supervisione fornite alle amministrazioni dovranno includere le succitate funzionalità

di consultazione ed esportazione di dati della Base Dati. Il servizio di stazione di supervisione include le relative attività di installazione e manutenzione. Alle amministrazioni con più di 20 accessi che ne facciano richiesta, una singola stazione di supervisione dovrà essere fornita gratuitamente.

Il NOC dovrà acquisire dalla sorgente situata presso il NOC QXN il Tempo Ufficiale della Rete (cfr. paragrafo 6.3.3) ed utilizzarlo come riferimento ai fini della marcatura con "time stamp" dei log e dei trouble ticket, nonché per tutte le altre funzioni di gestione della rete che richiedono un riferimento temporale.

Su richiesta dell'amministrazione o del CNIPA, il fornitore assegnatario dovrà, secondo procedure concordate, consentire l'accesso al NOC al personale incaricato del CG-SPC per effettuare verifiche sulle modalità di espletamento del servizio.

1.5.2 Misure di sicurezza dell'infrastruttura di connettività

Il fornitore assegnatario dovrà garantire che su tutte le infrastrutture utilizzate per l'erogazione dei servizi di connettività siano adottate le misure rispondenti ai requisiti minimi descritti nel seguito del presente paragrafo.

Il fornitore assegnatario dovrà nominare al suo interno un **Responsabile operativo locale della sicurezza** che dovrà fungere da punto di contatto prioritario per tutte le problematiche di sicurezza che interessano l'infrastruttura del fornitore assegnatario. Il Responsabile Operativo della sicurezza potrà avvalersi di sostituti i cui nominativi dovranno essere preventivamente comunicati al CG-SPC.

Misure generali:

- attuazione delle misure minime organizzative e tecniche previste dal Codice in materia di protezione dei dati personali (D.L. 30 giugno 2003, n. 196 Allegato B – Trattamento con strumenti elettronici);
- disposizione di un'organizzazione per la gestione della sicurezza dell'infrastruttura, secondo il modello indicato dalla norma BS7799-2;
- disposizione, nei punti di ingresso alle proprie infrastrutture utilizzate per l'erogazione dei servizi SPC, di sistemi di controllo e filtraggio del traffico (firewall e liste di controllo di accesso a protezione degli apparati router) e di verifica dell'assenza di codice malevolo nei messaggi di posta elettronica (antivirus);
- implementazione, sotto il controllo e la supervisione del CG-SPC, sul dispositivo che realizza il PAS sotto il proprio dominio amministrativo, di tutte le funzionalità volte ad impedire attacchi di tipo IP spoofing provenienti/diretti verso le reti dell'amministrazione;
- garanzia di tempestivo aggiornamento, con applicazione delle patch, del software/firmware degli apparati (router-switch) che trasportano il traffico destinato alle amministrazioni ed alla QXN, secondo le politiche stabilite dalla Commissione di Coordinamento del SPC;

- implementazione di un sistema di AAA centralizzato per l'autenticazione, l'autorizzazione e la tracciatura degli accessi sugli apparati di rete di propria competenza impiegati sul SPC.

Misure per il contrasto e recupero:

- controllo costante dei propri apparati di rete e della rete fisica di trasporto con lo scopo di individuare eventuali anomalie che possano essere sintomo di problemi di sicurezza;
- analisi automatica del traffico di rete con sistemi IDS (Intrusion Detection System) con l'obiettivo di riconoscere potenziali attacchi;
- attivazione delle funzioni di logging del traffico su tutti gli apparati di rete e sicurezza. I log dovranno essere conservati con modalità e tempi coerenti con le indicazioni del Codice della Privacy. I log relativi agli apparati di sicurezza dovranno essere analizzati giornalmente;
- definizione ed implementazione delle procedure di gestione degli incidenti a valle di segnalazioni di eventi di sicurezza.

Misure organizzative:

- analisi dei rischi su base sistematica, almeno con cadenza annuale. Tale analisi dovrà inoltre essere ripetuta a seguito di attacchi o incidenti gravi di sicurezza o per variazioni significative dell'architettura;
- verifica, con cadenza almeno semestrale, della capacità di resistenza del proprio spazio trasmissivo nei confronti di attacchi esterni;
- schedulazione di periodiche attività di revisione delle utenze e delle autorità di sicurezza ed immediata cancellazione delle utenze relative al personale che risolve il rapporto di lavoro;
- separazione delle responsabilità interne relative alla gestione della sicurezza ed alle verifiche;
- attivazione di un'organizzazione per la gestione dell'emergenza e dei problemi di sicurezza, volta ad assicurare la continuità del servizio nel caso di eventi eccezionali imprevedibili attraverso la stesura e la gestione dei piani per l'emergenza.

1.5.3 Call Center

Il fornitore assegnatario dovrà rendere disponibile alle amministrazioni un servizio di Call Center attivo H24, 7 giorni su 7, integrato con le strutture di NOC e SOC (cfr. paragrafo 1.5.1 , 2.12.1), costituito da un servizio di help-desk telefonico, ad opera di personale tecnico specializzato. Tale servizio dovrà essere configurato come un help desk di 2° livello, che riceve segnalazioni di malfunzionamento esclusivamente dai centri di gestione 1° livello della singola amministrazione, dal CG-SPC o dai NOC/SOC di altri fornitori assegnatari. L'utente finale della singola amministrazione potrà accedere direttamente al servizio di help desk di 1° livello, il quale dirotterà la segnalazione al 2° livello solo se rileverà un problema di competenza del fornitore assegnatario.

Il servizio di Call Center dovrà ricevere segnalazioni di malfunzionamento almeno tramite chiamata telefonica e tramite fax. Il fornitore assegnatario potrà integrare la struttura del Call Center tramite soluzioni basate su modalità web ed e-mail. Tuttavia queste soluzioni non saranno considerate sostitutive dell'accesso telefonico.

Per la ricezione delle chiamate il fornitore assegnatario dovrà istituire un apposito Numero Verde e dovrà predisporre attrezzature idonee in termini di apparati e linee al fine di garantire i livelli di

servizio definiti negli allegati 2c e 3a. Il fornitore assegnatario dovrà garantire la gestione di tutte le chiamate telefoniche e pertanto, nel caso di completa occupazione degli operatori del Call Center, dovrà attivare un sistema d'attesa che raccolga la segnalazione dell'amministrazione da notificare al primo operatore disponibile.

1.5.4 Servizi di Fault Management

Il call center del fornitore assegnatario dovrà erogare un servizio di fault management consistente nella rilevazione, diagnosi e risoluzione dei guasti occorrenti sui servizi di connettività. In particolare, per i malfunzionamenti che coinvolgono gli apparati installati presso i siti dell'amministrazione, il fornitore assegnatario dovrà intervenire secondo le seguenti modalità:

- gestione remota di tutti gli apparati installati presso i siti dell'amministrazione dal proprio NOC per la risoluzione dei malfunzionamenti;
- manutenzione on-site, qualora il malfunzionamento non permetta una correzione attraverso il supporto remoto. Le attività di fault management che richiedano intervento diretto sul sito dovranno essere effettuate nella finestra di erogazione del servizio e concordati con l'amministrazione.

Qualora una componente o parte di una componente del servizio di connettività installata presso i siti dell'amministrazione presenti un malfunzionamento, il fornitore assegnatario dovrà provvedere alla sua sostituzione secondo i tempi di ripristino del servizio descritti negli allegati 2c e 3a, in funzione del tipo di impatto provocato dal malfunzionamento.

L'amministrazione, qualora lo ritenga opportuno, potrà mettere a disposizione del fornitore, presso i propri siti, uno o più magazzini adatti allo spare-part management, secondo modalità che verranno concordate tra le parti.

Il fornitore assegnatario dovrà dotarsi di uno strumento di Trouble Ticketing per consentire la gestione ed il monitoraggio delle attvità di fault management, fermo restando che la classificazione del livello di severity dei TT sarà cura dell'amministrazione.

Anche il CG-SPC potrà aprire dei Trouble Ticket (TT) verso il fornitore assegnatario, a seguito di incongruenze nate dall'osservazione dei dati raccolti in maniera autonoma. Sarà compito del fornitore assegnatario mettere a disposizione del CG-SPC gli strumenti necessari per aprire i TT presso i propri sistemi.

L'apertura di un TT da parte di una amministrazione, afferente al fornitore X, può generare i seguenti casi:

- il problema segnalato è interno al fornitore X che lo risolve;
- il problema è interno alla QXN; il fornitore X inoltra il TT al NOC-QXN (cfr. paragrafo 1.5.1), che riconcilia eventuali TT aperti da altri fornitori relativamente allo stesso problema e lo risolve;
- il problema è interno al fornitore Y; il NOC-QXN inoltra il TT al fornitore Y, che lo risolve;
- nessuno degli attori coinvolti riconosce il problema come di sua competenza. In questo caso si dovrà provvedere all'escalation verso il CG-SPC che, grazie alle misurazioni indipendenti effettuate dalla **Terza Parte di Misura (TPM)**, può assegnare le corrette responsabilità.

L'escalation verso il CG-SPC potrà essere effettuata sia dal NOC-QXN, nel caso il problema non coinvolga ulteriori fornitori, sia dal fornitore.

Il fornitore assegnatario dovrà 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.

Il fornitore assegnatario dovrà garantire piena disponibilità ad integrare i sistemi di TT in maniera automatica con il CG-SPC e la QXN. Attraverso tale integrazione dovranno essere garantite almeno le funzioni principali per la gestione di un TT:

- apertura;
- chiusura;
- notifica.

Tale integrazione dovrà essere raggiunta attraverso XML per consentire l'interfacciamento di sistemi di Trouble Ticketing di diversi vendor.

1.5.5 Servizi di Provisioning, Configuration e Change Management

Il fornitore assegnatario dovrà installare e configurare opportunamente i servizi di connettività, così come definito precedentemente, fornendo all'amministrazione un servizio "chiavi in mano".

Il fornitore assegnatario dovrà erogare le seguenti prestazioni:

- attivazione e cessazione di nuovi servizi di connettività e delle relative componenti;
- installazione e configurazione degli apparati: il fornitore dovrà garantire l'effettiva installazione degli apparati per la fornitura dei servizi di connettività acquistati dall'amministrazione. Il fornitore dovrà consegnare all'amministrazione un inventario degli apparati installati;
- installazione del software: il fornitore dovrà farsi carico delle attività di installazione del software sugli apparati. Tale attività potrà essere realizzata presso i siti dell'amministrazione o presso i siti del fornitore stesso;
- trasloco completo dei servizi di connettività;
- variazione eventuale delle componenti dei servizi di connettività;
- variazione delle configurazioni dei flussi di traffico;
- attuazione degli adeguamenti, riconfigurazioni o ristrutturazioni richiesti da attività di "system tuning";
- caricamento ed attivazione di nuove release software sugli apparati della rete di trasporto e su tutti i sistemi utilizzati;
- aggiornamento software degli apparati per mantenere l'allineamento con i rilasci software messi a disposizione dai fornitori della tecnologia sia con finalità di patching che per quanto riguarda l'introduzione dei nuovi servizi;
- gestione remota degli apparati installati presso i siti dell'amministrazione che permetta al fornitore di intervenire dai propri NOC e SOC per attività operative;

Il fornitore assegnatario dovrà gestire e controllare tutte le configurazioni hardware e software degli apparati utilizzati per l'erogazione dei servizi, mantenendo aggiornato un database delle configurazioni (integrato con le Basi Dati di NOC e SOC) che consenta:

- l'inventario delle configurazioni hardware e software e delle personalizzazioni necessarie, in modo da facilitare le operazioni di ripartenza e riallineamento a fronte di un qualsiasi problema legato alle funzionalità dei sistemi gestiti;
- la produzione quadrimestrale di un report delle configurazioni;
- la pianificazione delle attività di gestione e di aggiornamento dei sistemi.

In particolare, la fornitura dei servizi di telefonia su IP (cfr. paragrafo 1.3), dovrà essere preceduta dalle seguenti attività di preparazione dell'installazione, a cura del fornitore assegnatario:

- verifica dei pre-requisiti tecnologici rispettati dall'infrastruttura di rete locale in cui verrà integrato il dominio VoIP. In particolare il fornitore assegnatario dovrà verificare i seguenti aspetti:
  - presenza di una rete locale Ethernet switched;
  - categoria del cablaggio di edificio (almeno UTP CAT-4);
  - possibilità di introdurre VLAN dedicate al traffico voce e alla segnalazione separate dalla VLAN dati;
- rilascio da parte del certificato per l'attestazione dell'idoneità delle infrastrutture messe a disposizione dall'amministrazione ai fini dell'erogazione dei servizi VoIP, nel rispetto dei SLA definiti negli allegati 2c e 3a.

1.5.6 Servizi di Rendicontazione

Il fornitore assegnatario dovrà 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 dell'amministrazione.

In caso di specifiche esigenze da parte dell'amministrazione in merito al formato dati, il fornitore assegnatario dovrà garantire la propria disponibilità a personalizzare la struttura della documentazione.

Il fornitore assegnatario dovrà garantire alle singole amministrazioni la disponibilità dei dati, sia analitici che sintetici, su supporto elettronico (almeno .xls e .csv).

Il fornitore assegnatario dovrà mettere a disposizione dell'amministrazione strumenti per la gestione e la consultazione tramite web dei dati di fatturazione e di rendicontazione. Tali strumenti dovranno essere aggiornati almeno mensilmente ed essere relativi ad almeno gli ultimi sei bimestri.

Il fornitore assegnatario dovrà altresì rendere disponibili i dati sopra descritti con frequenza bimestrale e dovrà indicare i tempi di fornitura dei primi dati di fatturazione per la singola amministrazione a partire dalla data di attivazione del servizio.

Il sistema di fatturazione del fornitore assegnatario dovrà fornire tutte le informazioni di dettaglio in merito alle sessioni tariffate, nel rispetto sulle norme della privacy in vigore. La fatturazione dovrà essere accompagnata da un report contenente informazioni relative all'erogazione di ogni singolo servizio, nel rispetto delle modalità e dei contenuti definiti negli allegati 2c e 3a.

Il fornitore aggiudicatario dovrà garantire per i servizi realizzati attraverso l'offerta OPO una rendicontazione analoga a quella prevista per l'offerta OPA ed articolata per amministrazione.

1.5.7 Servizi di Supporto sistemistico

Il fornitore assegnatario dovrà erogare alle amministrazioni il supporto necessario per la redazione del "Piano dei fabbisogni" (cfr. paragrafo 4.1) propedeutico alla definizione dei contratti esecutivi. Tale supporto dovrà consentire alle amministrazioni di valutare le opportunità offerte dai servizi SPC e di analizzare gli impatti tecnici ed organizzativi in relazione all'infrastruttura di rete pre-esistente presso la singola amministrazione.

1.5.8 Formazione

Il fornitore assegnatario dovrà erogare alle amministrazioni servizi di formazione. Le attività di formazione potranno essere svolte, a discrezione della amministrazione, e previo accordo tra quest'ultima ed il fornitore assegnatario:

- presso una sede centrale (modalità centralizzata) realizzata e attrezzata a carico del fornitore assegnatario presso una propria sede;
- presso i locali dell'amministrazione interessata (formazione decentrata); tutti gli oneri per l'allestimento delle sale attrezzate decentrate saranno a carico del fornitore assegnatario.

Il fornitore assegnatario dovrà redigere un Documento intitolato **"Piano di dettaglio di formazione"** (cfr. paragrafo 8.2) per singola amministrazione. Al suddetto piano dovranno essere allegati i curricula dei docenti.

Servizi di formazione di base

Il fornitore assegnatario dovrà presentare erogare servizi di formazione di base per le figure professionali che svolgono presso l'amministrazione un ruolo operativo di supervisione della rete e di help desk di primo livello per gli utenti.

I suddetti servizi dovranno tener conto delle necessità e delle conoscenze possedute dai destinatari delle attività di formazione e trattare argomenti che permettano di comprendere l'erogazione dei servizi SPC, l'organizzazione della QXN, la configurazione e l'esercizio della rete, le funzionalità offerte dalla stazione di supervisione, le problematiche di garanzia della qualità del servizio, le modalità di ripristino della funzionalità della rete oltre che una conoscenza di base di networking che comprenda almeno:

- modello ISO/OSI;
- protocollo Ethernet;
- protocollo IP;
- principali protocolli di trasporto (TCP, UDP) ed applicativi (FTP, HTTP, Telnet, etc.);
- principali architetture di rete in ambito locale (LAN) e geografiche (WAN);

- descrizione funzionale dei principali apparati di rete (hub, router, switch, etc.);
- introduzione alle VLAN e al protocollo IPSec.

I corsi di formazione saranno realizzati a classi che prevedano un numero di discenti pari a:

- 3-5 discenti per le amministrazioni con un numero di accessi superiore alle 15 unità;
- 1-3 discenti per amministrazioni con un numero di accessi non superiore alle 15 unità.

La durata dei corsi sarà concordata con l'amministrazione sulla base del programma formativo e sulla base del grado di conoscenza dei discenti ma non potrà superare i 3 gg lavorativi.

Il servizio di formazione dovrà essere svolto da personale qualificato, in possesso di almeno una certificazione in ambito networking.

Servizi di formazione specifici

Il fornitore assegnatario dovrà presentare, su richiesta dell'amministrazione, un progetto di formazione specifico per le risorse dell'amministrazione.

Gli argomenti dei corsi di formazione riguarderanno tematiche relative alle reti di telecomunicazione a alla sicurezza dei Sistemi Informativi, tra cui:

- protocolli evoluti (ad esempio: 802.1w, 802.1s, 802.1x);
- reti MPLS;
- gestione della QoS;
- soluzioni wireless e implementazione di reti Wi-Fi;
- sistemi e architetture VoIP;
- protocolli di Multicast.

I corsi di formazione saranno realizzati a classi che prevedano un minimo di 5 discenti ed un massimo di 10. Il numero delle sessioni e, conseguentemente, la durata dei corsi sarà concordata con l'amministrazione sulla base del programma formativo e sulla base del grado di conoscenza dei discenti.

2 SERVIZI DI SICUREZZA

2.1 Ambito di erogazione dei servizi

L'ambito di erogazione dei servizi di sicurezza SPC è costituito dal Sistema Informativo e relativa infrastruttura tecnologica sotto il dominio amministrativo della pubblica amministrazione e dalle infrastrutture telematiche ad essi interconnesse.

Relativamente a tali infrastrutture telematiche si distinguono:

- **Rete fidata (trusted)**: qualsiasi infrastruttura messa a disposizione da un fornitore di connettività SPC. Le infrastrutture di rete di un fornitore SPC e la QXN costituiscono tutte reti fidate e dovranno garantire il livello minimo di sicurezza previsto nel paragrafo 1.5.2 .
- **Rete non fidata (untrusted)***:* qualsiasi infrastruttura di rete, interconnessa a quella del Sistema Informativo della pubblica amministrazione, che non faccia parte del SPC.

2.2 Caratteristiche generali dei servizi

Il fornitore assegnatario dovrà erogare, su tutto il territorio nazionale, i servizi di sicurezza elencati nella tabella seguente:

Servizi di sicurezza SPC
• Firewall Management
• Antivirus & Content Filtering Management
• Network Intrusion Detection System Management
• Event & Log Monitoring Management
• VPN (in ambito SPC) Management
• Hardening dei sistemi
• Network Address Translation Management
• Host Intrusion Detection System Management
• Vulnerability Assessment

Tabella 14: Elenco dei servizi di sicurezza del SPC

2.2.1 Modalità di erogazione dei servizi

Il fornitore assegnatario dovrà erogare i servizi di sicurezza sopra elencati in modalità **"outsourcing completo**". Il fornitore assegnatario avrà pertanto la completa responsabilità della configurazione, amministrazione, monitoraggio e manutenzione delle componenti che realizzano i servizi e che possono essere di proprietà dell'amministrazione o del fornitore stesso.

All'amministrazione resterà la responsabilità di esprimere al fornitore assegnatario tutti i requisiti necessari per la corretta installazione e configurazione dei servizi e fornire tutte le informazioni di propria competenza per la configurazione dei servizi.

Il fornitore assegnatario dovrà collaborare con l'amministrazione nella gestione della politica di sicurezza nel quadro delle regole generali dettate per il SPC.

Tutti i dispositivi utilizzati per l'erogazione dei servizi di sicurezza dovranno integrare schemi di autenticazione attraverso i quali sia possibile l'accesso logico da console e da remoto.

Al riguardo potranno essere supportati uno o più meccanismi di autenticazione tra quelli riportati nella seguente tabella. In alternativa, potranno essere utilizzati anche altri schemi di autenticazione purché la comunicazione tra la stazione di gestione ed il dispositivo gestito sia cifrata.

Tipologia di autenticazione	Meccanismi di autenticazione
Da Console	• Server Radius; • ACE server; • password statiche configurabili sul dispositivo utilizzato; • password dinamiche generate per il tramite di token; • One Time Password (OTP).
Da remoto	• ACE server; • password dinamiche generate per il tramite di token; • One Time Password (OTP).

Tabella 15: Tipologia di autenticazione ai servizi di sicurezza del SPC

Il fornitore assegnatario dovrà erogare i servizi utilizzando apparati che si interfaccino con i sistemi dell'amministrazione attraverso interfacce conformi agli standard IEEE Ethernet/Fast-Ethernet/Gigabit-Ethernet. Sarà facoltà dell'amministrazione scegliere fra le sopra interfacce.

Il fornitore assegnatario avrà facoltà, nel rispetto delle prestazioni richieste dal presente capitolato tecnico, di erogare i servizi di trasporto e sicurezza tramite apparati integrati. Tuttavia, nel caso decida di avvalersi di un'offerta OPO, il fornitore assegnatario dovrà utilizzare modalità di erogazione del servizio che garantiscano la separazione degli apparati utilizzati per la fornitura dei servizi di connettività.

2.3 Firewall Management

2.3.1 Descrizione del servizio

Il fornitore assegnatario dovrà implementare e gestire sistemi di firewalling nelle due seguenti modalità:

- **network firewall**: si intende una configurazione hardware/software che realizza uno o più sistemi che sono interposti tra almeno una coppia di sottoreti IP. Un network firewall deve offrire protezione analizzando e filtrando all'occorrenza tutto il traffico che transita tra le reti tra cui è interposto.
- **personal firewall**: si intende una configurazione software che consente di proteggere le postazioni di lavoro da accessi indesiderati bloccando indirizzi, porte e protocolli.

I sistemi di firewalling su cui è basato il servizio dovranno supportare tutti i protocolli specificati nello standard TCP/IP e potranno essere realizzati per il tramite di uno o più dispositivi hardware/software eterogenei (un singolo router, una combinazione di router, un singolo sistema host o più host che eseguono un particolare software, dispositivi hardware progettati specificatamente per fornire le funzionalità di firewalling, una combinazione di essi). La selezione ed implementazione della tipologia di dispositivo di tipo firewall dipende dai requisiti dell'amministrazione.

I sistemi di firewalling su cui è basato il servizio dovranno supportare una politica di sicurezza di rete del tipo: "Nega qualsiasi servizio eccetto quelli esplicitamente permessi". In fase di installazione e messa in esercizio tutti i servizi dovranno essere temporaneamente bloccati e sarà possibile autorizzare i servizi necessari solo ad avvenuta installazione e verifica della corretta operatività del firewall.

Il fornitore assegnatario dovrà garantire le seguenti caratteristiche di base per il servizio di firewalling:

- **Filtraggio di traffico IP**: consente di proteggere una rete IP o singole postazioni di lavoro da accessi indesiderati bloccando indirizzi, porte e protocolli.
- **Auditing e logging**: consente l'analisi del traffico che attraversa il firewall.
- **Modulo di ispezione**: effettua l'ispezione dei datagrammi IP e realizza il filtraggio sulla base delle regole implementate. Dovrà essere implementata la metodologia "stateful inspection" escludendo l'impiego di dispositivi di firewalling del tipo Packet Filtering Stateless.
- **Modulo di gestione**: è il componente funzionale che consente di configurare e monitorare il comportamento del sistema firewall.

Su richiesta dell'amministrazione il fornitore assegnatario dovrà garantite le seguenti caratteristiche aggiuntive:

- **Gestione dell'autenticazione e controllo degli accessi**: consente di regolare l'impiego di alcuni servizi (FTP, Telnet, http, https) veicolati per il tramite del firewall sulla base di una preventiva autenticazione.
- **Port Address Translation (PAT) Management**: consente di nascondere, al fine di aumentare il livello di protezione, le porte effettive di ascolto di un sistema server protetto dal firewall, con porte fittizie.
- **URL Filtering Management**: consente di abilitare la navigazione WEB che avviene per il tramite del firewall solo a determinate postazioni, di controllare le statistiche sulla navigazione e di bloccare l'accesso a particolari siti Internet/Intranet.

2.3.2 Profili del servizio

Il fornitore assegnatario dovrà erogare i profili di servizio Network Firewall differenziati in base al numero dei segmenti di rete che devono essere dietro la protezione del firewall, al numero degli IP protetti ed al throughput, come riportato nella tabella seguente:

Profili di	Segmenti di rete	Numero Massimo	Throughput

servizio		di nodi IP	
FW-1	1 (nessuna DMZ)	25	Fino a 0,512 Mb/s
FW-2	2 di cui 1 DMZ	50	Fino a 2 Mb/s
FW-3	3 di cui 2 DMZ	100	Fino a 10 Mb/s
FW-4	Oltre 2 DMZ	illimitati	Oltre 10 Mb/s

Tabella 16: FW Management: profili di servizio di Network Firewall

Il fornitore assegnatario dovrà erogare i profili di servizio Personal Firewal, differenziati in base alle funzionalità erogate, elencati nella tabella seguente:

Profili di servizio	Funzionalità erogate
PFW-1	Semplice rilevazione delle porte e dello stato delle eventuali connessioni aperte su di esse; nessuna informazione sui servizi corrispondenti.
PFW-2	Associazione porta-servizio o protocollo, visualizzazione dei servizi connessi e stato delle connessioni**.**
PFW-3	Associazione porta-servizio-eventuale server software o deamon in attività sulla porta.
PFW-4	Port filtering statico, su configurazione predefinita del personal firewall e modificabile su esigenza dell'amministratore.
PFW-5	Port filtering dinamico, su configurazione service-based (es. per la gestione di servizi FTP, che fanno uso di porte dinamiche), su configurazione modificabile su richiesta dell'amministratore.
PFW-6	Filtro service-based con ACL (servizi accessibili in base ad Access Control List), su configurazione modificabile dall'amministratore locale o di dominio, o alternativamente da uno o più utenti esplicitamente abilitati.

Tabella 17: FW Management: profili di servizio di Personal Firewall

I servizi di Personal firewall dovranno essere erogati almeno sui seguenti sistemi operativi:

- Windows 2000 Professional;
- Windows 2000 Server/Advanced Sever/Data Center;
- Windows 2003 Server;
- Windows XP Home edition/Professional;
- Linux (kernel 2.2 o superiore);
- Mac OSX, MAC OS9;
- Unix (HP-UX, Sun Solaris, IBM AIX).

2.4 Antivirus & Content Filtering Management

2.4.1 Descrizione del servizio

Il fornitore assegnatario dovrà offrire un servizio di Antivirus & Content Filtering Management consistente nell'implementazione e gestione di un sistema di protezione del Sistema Informativo dell'amministrazione da spamming, da attacchi veicolati tramite il protocollo HTTP e da qualsiasi tipologia di codice software eseguibile (Virus, Worm, Cavallo di Troia, etc.) che può provocare danni al Sistema Informativo dell'amministrazione.

Il fornitore assegnatario dovrà implementare il sistema proposto come gateway del traffico IP mediante un'architettura di tipo proxy applicativo, in modalità bridge o router.

Il fornitore assegnatario dovrà garantire le seguenti caratteristiche del servizio di Antivirus & Content Filtering Management:

- **AVG - Antivirus Gateway.** Gestione di un sistema centralizzato per la protezione da codice dannoso che può propagarsi tramite lo scambio di posta elettronica; il fornitore assegnatario dovrà proporre un sistema caratterizzato dai seguenti parametri:
    - efficienza di scansione: 100% dei virus noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e dal media di trasmissione;
    - efficienza nel riparare file o messaggi infetti: 100% dei virus per i quali esiste la possibilità di recupero;
    - capacità di eseguire la scansione in tempo reale sui pacchetti IP;
    - capacità di eseguire la scansione differita di interi file/documenti allegati;
    - supporto 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 black list e riconoscimento di porzioni del contenuto del messaggio di posta elettronica personalizzabili;
    - supporto ai filtri di esclusione sul tipo di file trasferito in allegato (esempio: vbs, exe, pif, bat, etc.);
    - controllo sulla presenza di codice dannoso sui file allegati ai messaggi di posta elettronica supportando almeno i seguenti formati di dati:
        - file con diverse estensioni (vbs, exe, pif, bat);
        - file in formati compressi (zip, gzip, tgzip, rar);
    - verifica sintattica e semantica sull'header dei messaggi;
    - piena interoperabilità e/o trasparenza rispetto client e server;
    - 5 secondi di ritardo massimo introdotto per l'analisi di ogni singolo messaggio (riferito a messaggi di circa 2 Mbyte);
    - 1 secondo di ritardo medio introdotto per l'analisi di ogni singolo messaggio (riferito a messaggi di circa 200 Kbyte);
    - supporto dei protocolli standard: SMTP, POP vers. 3 e vers. 4, IMAP vers. 4.
- **HTTPG - HTTP Gateway.** Gestione di un sistema centralizzato 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; il fornitore assegnatario dovrà proporre un sistema caratterizzato dai seguenti parametri:

- efficienza di scansione: 99% dei virus noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e dal media di trasmissione;
- scansione in tempo reale sui pacchetti IP;
- supporto dei formati compressi (almeno zip, gzip, tgzip, rar);
- supporto ai filtri di esclusione sul tipo di file trasferito (esempio: vbs, exe, pif, bat, etc.);
- piena interoperabilità e/o trasparenza rispetto client e server;
- 2 secondi a Mbyte di ritardo massimo introdotto;
- supporto di protocolli standard: HTTP, HTTPS.

- **FTPG - FTP Gateway.** Gestione di un sistema centralizzato per la protezione da codice dannoso che può propagarsi per il tramite del trasferimento di file mediante FTP; il fornitore assegnatario dovrà proporre un sistema caratterizzato dai seguenti parametri:
  - efficienza di scansione: 100% dei virus noti, recensiti e pubblicamente elencati dalle organizzazioni preposte, indipendentemente dalla piattaforma ospite e dal media di trasmissione;
  - scansione in tempo reale sui pacchetti IP;
  - supporto dei formati compressi (almeno zip, gzip, tgzip, rar);
  - piena interoperabilità e/o trasparenza rispetto client e server;
  - 5 secondi a Mbyte di ritardo massimo introdotto;
  - supporto di protocolli standard: FTP, FTPS.

Il fornitore assegnatario dovrà erogare il servizio di Antivirus & Content Filtering Management per i seguenti sistemi operativi:

- Windows 2000 Professional, Windows 2000 Server/Advanced Sever/Data Center;
- Windows 2003 Server;
- Windows XP Home edition/Professional;
- Linux (kernel 2.2 o superiore);
- Mac OSX, MAC OS9 ;
- Unix (HP-UX, Sun Solaris, IBM AIX).

Per tutti i sistemi di gateway proposti, il fornitore assegnatario dovrà assicurare la gestione delle “firme di definizione del codice dannoso” e delle “signature” e garantirne l’aggiornamento sia con periodicità almeno mensile, sia su richiesta dell’amministrazione.

Su richiesta dell’amministrazione il fornitore assegnatario dovrà inoltre garantire le seguenti componenti del servizio:

- installazione e prima configurazione del software antivirus su host (posti di lavoro e sistemi server) indicati dall’amministrazione;

- gestione centralizzata del software antivirus installato su host dell'amministrazione;
- supporto e assistenza all'utilizzo ed alle successive configurazioni/aggiornamenti del software antivirus installato su host dell'amministrazione.

2.4.2 Profili del servizio

Il fornitore assegnatario dovrà erogare i profili di servizio di Antivirus & Content Filtering Management, elencati nella tabella seguente, differenziati in base alle seguenti caratteristiche:

- throughput supportato in messaggi al secondo[1];
- throughput supportato in Mb/s.

Profili di servizio	Throughput in messaggi al secondo	Throughput in Mb/s
AVG-1	25	
AVG-2	50	
AVG-3	100	
AVG-4	300	
AVG-5	1000	
AVG-6	fino a 5000	
HTTP-1		Fino a 0,512 Mb/s
HTTP-2		Fino a 2 Mb/s
HTTP-3		Fino a 10 Mb/s
HTTP-4		Oltre 10 Mb/s
FTP-1		Fino a 0,512 Mb/s
FTP-2		Fino a 2 Mb/s
FTP-3		Fino a 10 Mb/s
FTP-4		Oltre 10 Mb/s

Tabella 18: Antivirus & Content Filtering Management - profili di servizio

2.5 Network Intrusion Detection System (NIDS) Management

2.5.1 Descrizione del servizio

Il fornitore assegnatario dovrà erogare un servizio consistente nell'implementazione e gestione di sistemi di rilevamento delle intrusioni (Network Intrusion Detection System, NIDS) che consenta di identificare positivamente 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 fornitore assegnatario dovrà erogare il servizio di NIDS Management tramite i seguenti componenti funzionali:

[1] Messaggi da 200 Kbyte in media.

- **Sensore**: raccoglie dati dalla rete (pacchetti dati) e li inoltra all'Analyzer. I sensori devono poter monitorare segmenti di rete con prestazioni pari a 10 Mb/s (Ethernet), 100 Mb/s (Fast-Ethernet) e 1000 Mb/s (Gigabit Ethernet).
- **Analyzer**: riceve input da uno o più sensori o da altri analyzer, e determina l'occorrenza di una situazione di attacco. L'output di questo componente rappresenta un'indicazione di avvenuta intrusione da cui possono scaturire azioni automatiche configurabili (almeno definizione policy su firewall, terminazione connessioni TCP, generazione trap SNMP).
- **User interface (o manager)**: consente di controllare e monitorare il comportamento del sistema NIDS.

Il fornitore assegnatario dovrà erogare un servizio di NIDS Management con le seguenti funzionalità:

- supporto dei protocolli IEEE Ethernet, Fast-Ethernet, Gigabit Ethernet e tutti i protocolli specificati nello standard TCP/IP.
- analisi passiva di un protocollo tramite l'uso di sniffer;
- capacità di rilevazione degli attacchi garantendo la percentuale di falsi positivi e falsi negativi definita negli allegati 2c e 3a.
- raccolta e conservazione tracce accurate degli avvenuti attacchi allo scopo di favorire l'individuazione degli autori dell'attacco e come deterrente per scoraggiare ulteriori azioni ostili;
- raccolta di informazioni sugli eventi di attacco da una o più sorgenti di informazione tramite "sensori" posti sulla rete;
- analisi predeterminata degli eventi rilevati attraverso l'utilizzo di "signature analysis" che consentono 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;
- gestione del database delle "signature". Il fornitore assegnatario dovrà aggiornare sia con periodicità almeno mensile, sia su richiesta dell'amministrazione, le "signature" dei sistemi NIDS per mezzo dei quali viene erogato il servizio;
- esecuzione della "forensic analysis" degli attacchi;
- notifica specifica a fronte dell'identificazione di un evento di attacco;
- notifica all'amministrazione di eventuali situazioni che necessitino di interventi/decisioni da parte dell'amministrazione stessa;
- definizione di regole personalizzate per:
    - tener conto di eventuali vulnerabilità riscontrabili mediante un'attività di risk assessment effettuata sulla Intranet dell'amministrazione;
    - registrare le attività sulla rete che rispondono a determinate condizioni;
    - attivare delle notifiche a fronte di particolari sequenze di eventi sulla rete;
    - attivare delle azioni specifiche di contrasto all'intrusione personalizzabili.

2.5.2 Profili del servizio

Il fornitore assegnatario dovrà erogare profili di servizio differenziati in base alle seguenti caratteristiche:

- numero e tipologia dei segmenti di rete su cui monitorare il traffico;
- throughput del traffico analizzato;
- classe di attacchi.

Il fornitore assegnatario dovrà erogare i profili di servizio di NIDS Management elencati nella tabella seguente:

Profili di servizio	Segmenti di rete	Throughput	Classe di attacchi
NIDS-1	esterno	Fino a 0,512 Mb/s	3, 4
NIDS-2	Da 1 a 4	Fino a 2 Mb/s	3, 4
NIDS-3	Da 1 a 4	Fino a 10 Mb/s	2, 3, 4
NIDS-4	Da 1 a 8	Oltre 10 Mb/s	1, 2, 3, 4

Tabella 19: NIDS Management: profili di servizio

La segmentazione in classi degli attacchi rilevabili dal servizio di NIDS Management è riportata nella tabella seguente:

Classe			
1	Accesso illegale a root dall'esterno ed utilizzo delle tecniche definite in "Accesso non autorizzato a risorse"		
2	Accesso illegale come utente dall'esterno ed utilizzo delle tecniche definite in "Accesso non autorizzato a risorse"		
3	DOS	Flooding	Ping flood
			Smurf
			SYN flood
			Spoofing (ip address falsificato)
			IP Source Routing
			Distributed DOS

		Vulnerabilità	Buffer overflow
			Configurazioni di default
			Ping of death
			Remote system shutdown
4	Accesso non autorizzato a risorse	Password cracking e violazione d'accesso	
		Cavalli di troia	
		Intercettamenti (flooding, hijacking, man-in-the-middle)	
		Spoofing (falsificazione di identità)	
	Probe	Port and services scanning	
		Rilevamento da remoto del sistema operativo	
		Connessione non autorizzata alla rete del sistema	

Tabella 20: NIDS Management – classificazione degli attacchi

2.6 Event & Log Monitoring Management

2.6.1 Descrizione del servizio

Il fornitore assegnatario dovrà provvedere alla raccolta, verifica, correlazione, analisi e storicizzazione degli allarmi generati e delle informazioni raccolte nei file di log dalle piattaforme caratterizzanti il sistema di sicurezza di cui dispone l'amministrazione. Il servizio dovrà permettere il monitoraggio del livello di sicurezza raggiunto all'interno dell'amministrazione.

Il fornitore assegnatario dovrà erogare un servizio di Event & Log Monitoring Management caratterizzato dalle seguenti caratteristiche:

- Supporto alla sorveglianza ed alla gestione degli allarmi. La piattaforma utilizzata per l'erogazione del servizio dovrà fornire le seguenti funzionalità:
    - recuperare le informazioni (log, allarmi ed eventi di sicurezza) generate dagli strumenti che realizzano il sistema di sicurezza dell'amministrazione. La piattaforma dovrà supportare gli standard: SNMP, MIB-I, MIB-II, RMON, RMON 2 e dovrà integrare e gestire MIB proprietarie. Il sistema dovrà gestire la ricezione di trap asincrone standard (ColdStart, WarmStart, LinkDown, LinkUP, AuthenticationFailure, EgpNeighborLoss) e quelle specifiche definite dai costruttori degli apparati gestiti;

- offrire la possibilità di convogliare tutti gli eventi/allarmi generati verso un unico punto di correlazione;
- analizzare e correlare le informazioni raccolte e presentarle, a valle di una normalizzazione, tramite un'interfaccia grafica e mediante generazione di un report di sintesi secondo dei template definibili sulla base delle specifiche esigenze dipendenti dalle tecnologie degli elementi gestiti;
- configurare la notifica di eventi/allarmi a fronte del superamento di soglie prefissabili e a seguito del verificarsi di eventi critici che impattano sulla sicurezza dell'ambiente informatico dell'amministrazione;
- assegnare differenti priorità agli eventi/allarmi e fornire, per ogni notifica ricevuta, informazioni circa:
  - la sorgente dell'evento/allarme;
  - la tipologia dell'evento/allarme;
  - la descrizione dell'evento/allarme;
  - la severità dell'evento/allarme;
  - l'istante temporale in cui si è verificato l'evento/allarme;
  - gruppo di appartenenza dell'evento/allarme;
  - ulteriori informazioni descrittive dell'evento/allarme, della risorsa che lo ha generato e di eventuali azioni automatiche o predefinite eseguite o disponibili;
- offrire la possibilità di reinstradamento dei messaggi di allarme e degli eventi a sistemi esterni, quali almeno:
  - trouble ticketing;
  - e-mail;
  - pager;
  - SMS su GSM;
- essere integrabile con:
  - sistemi di trouble ticketing;
  - tool di reporting;
  - prodotti di supporto alle attività di help desk;

- Gestione dell'inventario e storicizzazione dei dati. La piattaforma utilizzata per l'erogazione del servizio dovrà consentire la creazione ed il mantenimento di un inventario aggiornato degli strumenti (hardware e software) che realizzano il sistema di sicurezza dell'amministrazione e da cui sono prelevati log ed eventi/allarmi. La piattaforma dovrà soddisfare i seguenti requisiti:
  - inventariare e mantenere in una base di dati le informazioni sulle risorse che realizzano il sistema di sicurezza dell'amministrazione e contestualmente i log ed eventi/allarmi da essi generati e prelevati;
  - storicizzare le informazioni inventariate in database relazionali ed in formato noto;
  - personalizzare le informazioni inventariate tra cui:
    - locazione fisica del sistema di sicurezza da cui sono prelevati log ed eventi/allarmi;

        - nome, unità organizzativa e recapito dell'amministratore del sistema;
        - l'insieme dei servizi e delle funzionalità di sicurezza attivate sul sistema;
    - offrire modalità di accesso all'inventario tramite Command Line Interface (CLI), Application Program Interface (API) e Graphical User Interface (GUI);
    - evidenziare le differenze tra inventari successivi;
    - effettuare ricerche sulle informazioni inventariate mediante filtri e query personalizzabili.
- Rappresentazione dei dati elaborati. La piattaforma dovrà offrire la possibilità di rappresentare graficamente i dati contenuti nei log raccolti dagli strumenti che realizzano il sistema di sicurezza dell'amministrazione e dei dati elaborati e correlati a partire da quelli raccolti consentendo:
    - la generazione di grafici statistici run time, periodicamente o a seguito di eventi (ad esempio, produzione di un report ogni qual volta viene superata una soglia di allarme preconfigurata);
    - la consultazione dei dati attraverso browser HTTP;
    - la generazione di report e l'esportazione dei dati raccolti in vari formati (ad esempio: HTML, .csv, .xls, .txt, etc.);
    - la schedulazione degli intervalli di produzione dei report.

Il fornitore assegnatario inoltre dovrà erogare, su richiesta dell'amministrazione, le seguenti funzionalità:

- includere componenti software distribuite in grado di:
    - minimizzare il traffico indotto dall'esportazione remota delle console grafiche;
    - liberare la CPU della stazione di management principale dalla gestione dei processi della GUI;
- offrire la possibilità di replicare i dati memorizzati nei database.

2.6.2 Profili del servizio

Il fornitore assegnatario dovrà erogare i profili di servizio di Event & Log Monitoring Management differenziati, come mostrato nella tabella successiva, in base alle seguenti caratteristiche:

- numero massimo di dispositivi monitorati (sono i dispositivi da cui la piattaforma utilizzata per l'erogazione del servizio riceverà i log e le trap SNMP);
- entità del throughput previsto;
- Gbyte di dati memorizzati.

Profili di servizio	Numero Massimo di Dispositivi Monitorati	Throughput	Gbyte di eventi memorizzati
E&LM-1	64	Fino a 0,512 Mb/s	160 GB
E&LM-2	128	Fino a 2 Mb/s	320 GB
E&LM-3	512	Fino a 10 Mb/s	640 GB

E&LM-4	superiore a 512	Oltre 10 Mb/s	1000 GB

Tabella 21: Event & Log Monitoring: profili di servizio

2.7 VPN Management

2.7.1 Descrizione del servizio

Il fornitore assegnatario dovrà erogare un servizio di VPN Management consistente nella implementazione e nella gestione di reti virtuali private basate sullo standard IPSec come definito dall'IPSec Working Group dell'IETF (RFC 2401).

Il fornitore assegnatario dovrà erogare un servizio caratterizzato dalle seguenti caratteristiche:

- **Data Origin Authentication**: verifica l'autenticità del mittente di ciascun datagramma IP;
- **Data integrity**: 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**: nasconde il testo in chiaro contenuto in un messaggio, mediante l'impiego della crittografia;
- **Replay protection**: assicura che un hacker, intercettato un datagramma IP, non sia in grado, a posteriori, di rispedirlo a destinazione per qualche scopo illecito.

2.7.2 Modalità di erogazione del servizio

Il fornitore assegnatario dovrà erogare il servizio di VPN Management secondo una delle seguenti modalità:

- **autonoma**: il fornitore assegnatario dovrà provvedere alla realizzazione e gestione di entrambe le terminazioni dei tunnel che realizzano la VPN dell'amministrazione;
- **cooperativa***:* il fornitore assegnatario dovrà 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 assegnatario sia dettata dall'amministrazione che eroga i servizi applicativi. Le altre amministrazioni per poter usufruire i servizi su VPN IPSec richiedono il servizio di VPN Management allo stesso fornitore assegnatario. Sarà pertanto responsabilità del fornitore assegnatario la progettazione e la fornitura del servizio.

Topologia delle connessioni

Nel seguito sono descritte le possibili modalità di connessione di riferimento per il servizio IPSec che il fornitore assegnatario dovrà implementare su richiesta delle amministrazioni.

Connessione gateway-to-gateway

In questa modalità operativa il servizio offerto dovrà operare creando un tunnel tra due gateway secondo i meccanismi "tunnel mode" descritti nella specifica pubblica RFC 2401. I dispositivi gateway possono essere di tipo hardware e specifici per tale servizio o di tipo software installato su una TdR dell'amministrazione. È facolta dell'amministrazione richiedere dispositivi gateway di tipo hardware specifici per tale servizio.

Il fornitore assegnatario sarà completamente responsabile dell'erogazione dei servizi in modalità autonoma o predefinita, mentre il servizio, erogato in modalità cooperativa, richiederà l'implementazione e gestione dell'estremità dei tunnel sotto il dominio amministrativo del fornitore assegnatario, oltre a tutte le attività necessarie ad attivare il tunnel con fornitori terzi che gestiscono l'altra estremità. La modalità cooperativa richiederà che il fornitore impieghi sistemi interoperabili con terminazioni di tunnel diverse, gestite da fornitori terzi.

Connessione host-to-host

Il servizio dovrà operare creando un collegamento virtuale protetto secondo la modalità standard IPSec "transport mode" come descritta in RFC-2401. Il fornitore assegnatario dovrà fornire la specifica tecnica del prodotto offerto.

Il prodotto dovrà essere fornito almeno per le seguenti piattaforme: Windows-2000, Windows-XP, Linux (kernel 2.2 o superiore), Mac OSX e MAC OS9.

Connessione per l'accesso remoto (host esterno-gateway)

Il servizio dovrà operare creando un tunnel tra il nodo interessato ed un gateway della rete, secondo la modalità standard IPSec "tunnel mode" come descritta in RFC-2401.

Il fornitore assegnatario dovrà fornire le caratteristiche relative al client e al gateway terminatori del tunnel.

La parte client dovrà essere fornita almeno per le seguenti piattaforme: Windows-2000, Windows-XP, Linux (kernel 2.2 o superiore), Mac OSX e MAC OS9.

2.7.3 Profili del servizio

Il fornitore assegnatario dovrà erogare i profili di servizio di VPN Management differenziati, come mostrato nella tabella successiva, in base alle seguenti caratteristiche:

- numero massimo di tunnel contemporanei;
- entità del throughput cifrato previsto.

Profili di servizio	Numero Massimo Tunnel contemporanei	Throughput Cifrato
VPN-1	5	Fino a 0,512 Mb/s
VPN-2	50	Fino a 2 Mb/s
VPN-3	100	Fino a 10 Mb/s
VPN-4	1000	Oltre 10 Mb/s

Tabella 22: VPN Management - profili di servizio

Requisiti sul servizio

Relativamente all'autenticazione dei nodi ed alla gestione delle associazioni di sicurezza, la creazione e la negoziazione delle associazioni di sicurezza (SA, Security Association) del sistema IPSec dovranno essere garantite attraverso i meccanismi identificati dal protocollo Internet Key Exchange (IKE) secondo la specifica pubblica RFC 2409. Tali meccanismi dovranno supportare sia l'autenticazione mediante segreto condiviso ("pre-shared key") che quella mediante certificati digitali conformi allo standard ISO/IES 9594-8 (X.509v3).

L'impiego dei certificati digitali è obbligatorio qualora il servizio fosse erogato in modalità cooperativa.

2.8 Hardening dei sistemi

2.8.1 Descrizione del servizio

Il fornitore assegnatario dovrà erogare un servizio di Hardening dei sistemi consistente nello svolgimento delle attività elencate nel seguente piano di interventi:

- **Analisi dell'ambiente.** Analisi dettagliata delle vulnerabilità del Sistema Informativo dell'amministrazione e indicazione delle possibili contromisure; durante questa fase il fornitore assegnatario dovrà:
  - pianificare e sintetizzare gli adeguamenti di sicurezza previsti per i sistemi analizzati;
  - valutare l'adeguatezza degli aggiornamenti proposti e gli impatti sui sistemi di produzione;
  - pianificare e reperire le patch di sicurezza da installare;
  - sintetizzare e predisporre piani di ripristino.
- **Intervento e distribuzione patch.** Durante questa fase il fornitore assegnatario dovrà:
  - pianificare e concordare con l'amministrazione la necessità di eseguire determinate operazioni prima di distribuire l'aggiornamento;
  - definire un piano di attività e modalità di test;
  - definire e gestire l'ambiente di test;
  - gestire il rilascio ed il supporto delle configurazioni sicure, preventivamente verificate con successo mediante test;
  - concordare con l'amministrazione un piano di rilascio delle configurazioni e patch;
  - adeguare il software di base e applicativo in relazione alle vulnerabilità riscontrate con interventi di riconfigurazione;
  - installare le patch di protezione raccomandate dai produttori o da terzi volte ad eliminare le vulnerabilità che possono essere sfruttate per un attacco ai sistemi;
- **Monitoraggio e verifica.** Nell'ambito dei processi continuativi il fornitore assegnatario dovrà controllare regolarmente le nuove patch rilasciate, le nuove configurazioni effettuate sull'ambiente in esercizio e le contromisure necessarie alla messa in sicurezza del Sistema Informativo dell'organizzazione dell'amministrazione.

2.8.2 Profili del servizio

Il fornitore assegnatario dovrà erogare, per ogni sistema sottoposto ad hardening, i profili di servizio differenziati, come mostrato nella tabella successiva, in base alle seguenti caratteristiche:

- "una tantum" comprensiva anche delle attività di test e collaudo delle modifiche effettuate;
- con monitoraggio continuativo con periodicità mensile.

Profili di servizio	Modalità di erogazione Una tantum (UT) o Continuativa (CON)
H-UT	UT
H-CON	CON

Tabella 23: Hardening dei sistemi - profili di servizio

2.9 Network Address Translation Management

2.9.1 Descrizione del servizio

Il fornitore assegnatario dovrà erogare un servizio di Network Address Translation (NAT) Management consistente nella progettazione, implementazione e gestione di regole di traduzione di indirizzi IP configurati all'interno dell'infrastruttura di rete dell'amministrazione. Il servizio proposto dovrà essere tale da consentire di:

- nascondere i dettagli dell'indirizzamento utilizzato all'interno di una rete quando ci si connette da quella rete verso altre reti ritenute non fidate;
- convertire un pool di indirizzi IP utilizzati per la rete Intranet dell'amministrazione in un pool di indirizzi IP pubblici utilizzabili per l'accesso al SPC.

2.9.2 Modalità di erogazione del servizio

Il fornitore assegnatario dovrà articolare il servizio di NAT Management nelle seguenti fasi:

- analisi dei requisiti utente;
- analisi del piano di indirizzamento a cui vanno applicate le traduzioni di indirizzi;
- studio delle caratteristiche dei dispositivi che dovranno effettuare la traduzione degli indirizzi, limitatamente alle funzionalità a supporto del "natting";
- sintesi del piano di "natting";
- implementazione del piano di "natting", ove applicabile.

Il fornitore assegnatario dovrà erogare il servizio di NAT Management assicurando le attività di progettazione, attivazione, manutenzione e gestione del piano di indirizzamento.

2.9.3 Profili del servizio

Il fornitore assegnatario dovrà erogare i profili del servizio di NAT Management differenziati, come mostrato nella tabella successiva, in base alle tipologie di regole di traduzione degli indirizzi elencate nella tabella seguente:

Profili di servizio	Funzionalità erogate
NAT-NxN-S	NAT statico del tipo n<->n: ciascun indirizzo IP, appartenente al range a cui s'intende applicare il NAT, viene tradotto in un indirizzo IP distinto, appartenente ad un pool di indirizzi predeterminato. La corrispondenza indirizzo IP<->indirizzo IP tradotto è permanente, ovvero ogni indirizzo IP viene tradotto sempre in un medesimo indirizzo IP prelevato dal pool.
NAT-NxN-D	NAT dinamico del tipo n<->n: la corrispondenza indirizzo IP<->indirizzo IP tradotto è variabile, ovvero ogni indirizzo IP viene tradotto in un indirizzo IP libero, ovvero non già precedentemente assegnato dal NAT, prelevato dal pool degli indirizzi IP configurati per il NAT.
NAT-Nx1	Traduzione del tipo n<->1: ciascun indirizzo appartenente al range a cui s'intende applicare il NAT viene tradotto in un medesimo indirizzo IP predeterminato.

Tabella 24: NAT Management: profili di servizio

2.10 Host Intrusion Detection System (HIDS) Management

2.10.1 Descrizione del servizio

Il fornitore assegnatario dovrà erogare un servizio di Host Intrusion Detection System (HIDS) Management consistente nell'installazione e gestione di software specifico per il rilevamento delle intrusioni su sistemi server e postazioni di lavoro.

Il fornitore assegnatario dovrà garantire che il sistema HIDS impiegato per l'implementazione del servizio sia realizzato attraverso i seguenti componenti funzionali:

- **Sensore**: componente che raccoglie dati dall'host. L'input di un sensore può venire da ogni fonte di informazione che può contenere le prove di un'intrusione (file di log, processi attivi, porte TCP/IP in ascolto). I sensori raccolgono le informazioni e le inoltrano all'Analyzer.
- **Analyzer**: componente funzionale che, ricevendo input da uno o più sensori, determina l'occorrenza di una situazione di attacco. Di conseguenza l'output di questo componente è un'indicazione di avvenuta intrusione a cui possono scaturire azioni automatiche configurabili (almeno definizione policy su firewall, terminazione connessioni TCP, generazione trap SNMP).
- **User interface (o manager)**: componente funzionale che consente di controllare e monitorare il comportamento del sistema HIDS.

Il fornitore assegnatario dovrà garantire un servizio di HIDS Management che consenta la protezione dell'host attraverso le seguenti funzionalità:

- raccolta e conservazione delle tracce accurate degli avvenuti attacchi allo scopo di favorire l'individuazione degli autori dell'attacco e come deterrente per scoraggiare ulteriori azioni ostili;

- ottenimento di informazioni sugli eventi di attacco da una o più sorgenti di informazione tramite “sensori” posti sulla rete;
- esecuzione di un'analisi predeterminata degli eventi rilevati;
- esecuzione della “forensic analysis” degli attacchi dei sistemi server;
- generazione di una notifica specifica a fronte della identificazione di un evento di attacco;
- registrazione delle attività sull’host che rispondono a determinate condizioni;
- attivazione di regole personalizzabili per tener conto di eventuali vulnerabilità riscontrabili mediante un’attività di risk assessment effettuata sulla intranet dell’amministrazione;
- supporto, almeno, dei seguenti sistemi operativi:
    - Windows 2000 Professional
    - Windows 2000 Server/Advanced Sever/Data Center
    - Windows 2003 Server
    - Windows XP Home edition/Professional
    - Linux (kernel 2.2 o superiore)
    - Mac OSX, MAC OS9
    - Unix (HP-UX, Sun Solaris, IBM AIX).

2.10.2 Profili del servizio

Il fornitore assegnatario dovrà erogare i seguenti profili del servizio di HIDS Management:

HIDS-SO (HIDS per sistema operativo).

- Profilo A (protezione base):
    - rilevazione giornaliera della modifica di file di configurazione, elenco utenti del sistema e privilegi loro concessi;
- Profilo B (protezione intermedia), comprende il profilo A più:
    - rilevazione e blocco dei tentativi di esecuzione di processi con permessi differenti da quelli dell’utente abilitato;
- Profilo C (alta protezione), comprende il profilo B più:
    - rilevazione e blocco dei processi utente non autorizzati;
    - controllo di esecuzione dei processi del sistema prima dell’effettivo accesso alla risorsa richiesta;

HIDS-PDL (HIDS per postazione di lavoro).

- Profilo A (protezione di base):
    - servizio antivirus centralizzato (con periodico aggiornamento delle signature in modalità push);
- Profilo B (protezione intermedia), comprende il profilo A più:
    - servizio antivirus centralizzato (con periodico aggiornamento delle signature in modalità push);

    - personal firewall con configurazione non restrittiva (blocco di operazioni e servizi non standard, ma possibilità di modifica della configurazione da parte dell'utente abilitato);
    - software per l'amministrazione di sistema da remoto (con conseguente controllo dell'integrità della configurazione);
- Profilo C (alta protezione), comprende il profilo B più:
    - personal firewall con configurazione restrittiva (blocco di operazioni e servizi non standard, gestione e aggiornamento della configurazione non concessi all'utente);
- Profilo D (controllo completo del sistema), comprende il profilo B più:
    - sistema di controllo completo e remotizzato del sistema; creazione di profili utente vincolati (esecuzione di ben precise applicazioni, accesso a parti limitate dell'hard disk, rimozione dei privilegi di modifica e visione della configurazione di sistema e dei servizi);
    - sistema di aggiornamento forzato del sistema mediante creazione di immagini del disco fisso, backup remoto delle immagini e sovrascrittura dell'hard disk in caso di evento catastrofico o violazione di sicurezza;

HIDS-DB (HIDS per sistemi database).

- Profilo A (protezione di base):
    - rilevazione giornaliera della modifica dei file di configurazione del database; elenco utenti del database e privilegi loro concessi;
- Profilo B (protezione medio-alta), comprende il profilo A più:
    - filtro delle query in ingresso al database, per eliminare quelle esplicitamente malformate o dannose al sistema, che creino ad esempio inutile spreco di cicli di CPU, o ancora palesemente "indovinate" tentando di recuperare risorse con nomi di default;

HIDS-WEB (HIDS per sistemi Web).

- Profilo A (protezione di base):
    - rilevazione giornaliera dell'integrità di file di configurazione, script ed eseguibili esposti nella radice del file system contenente il codice software del servizio applicativo;
    - elenco degli utenti del sistema e privilegi loro concessi;
- Profilo B (protezione intermedia), comprende il profilo A più:
    - controllo e filtro delle richieste HTTP malformate (es. contenenti codice di exploit di vulnerabilità di tipo buffer overflow);
- Profilo C (alta protezione), comprende il profilo B più:
    - controllo e filtro del contenuto delle transazioni client-server verso le applicazioni ospitate dal server Web, per eliminare valori non accettabili, cookie riutilizzati illecitamente, etc.

2.11 Vulnerability Assessment

2.11.1 Descrizione del servizio

Il fornitore assegnatario dovrà erogare un servizio di Vulnerability Assessmnent consistente nell'analisi dell'esposizione al rischio di attacchi informatici delle risorse informatiche e telematiche del Sistema Informativo dell'amministrazione. Il servizio dovrà essere erogato mediante l'effettuazione di una serie di test condotti sia con l'ausilio di strumenti automatici che utilizzando i comandi propri del sistema operativo di base dei dispositivi oggetto di valutazione. I test automatici dovranno prevedere:

- la scansione dei dispositivi di rete, dei sistemi server e delle postazioni di lavoro alla ricerca di configurazioni del software di base e applicativo ritenute non sicure e vulnerabili ad attacchi;
- test di penetrazione che consentono di valutare la resistenza della rete, dei sistemi e delle postazioni di lavoro a determinati attacchi informatici simulati.

Al termine delle attività di Vulnerability Assessment il fornitore assegnatario dovrà redigere un documento di report sulle vulnerabilità accertate, indicante anche le possibili contromisure, che possa consentire all'amministrazione di verificare l'adeguatezza della politica di sicurezza implementata all'interno del proprio dominio di responsabilità e di adottare eventuali adeguamenti. Tutte le vulnerabilità dovranno essere catalogate secondo un metodo di valutazione quantitativo e qualitativo che permetta una precisa categorizzazione dei risultati e delle contromisure suggerite.

2.11.2 Profili del servizio

Il fornitore assegnatario dovrà erogare i profili del servizio di Vulnerability Assessment differenziati, come mostrato nella tabella successiva, in base alle seguenti caratteristiche:

- numero IP sui quali è effettuata l'analisi di vulnerabilità;
- modalità di erogazione:
  - "una tantum";
  - cadenza bimestrale.

Profili di servizio	Numero Massimo di nodi sotto Assessment	Erogazione Una tantum (UT) o Erogazione Bimestrale
VA-UT-1	1	UT
VA-UT-2	5	UT
VA-UT-3	10	UT
VA-UT-4	20	UT
VA-UT-5	50	UT
VA-BIM-1	1	BIM
VA-BIM-2	5	BIM
VA-BIM-3	10	BIM
VA-BIM-4	20	BIM
VA-BIM-5	50	BIM

Tabella 25: Vulnerability Assessment - profili di servizio

2.12 Manutenzione e assistenza dei servizi di sicurezza

Nell'ambito dei servizi di sicurezza il fornitore assegnatario dovrà erogare anche i relativi servizi di manutenzione e assistenza, i quali dovranno comprendere tutte le attività di gestione dei sistemi e della rete finalizzate a controllare ed intervenire a fronte di anomalie su tutte le componenti dei servizi offerti:

- installazione, attivazione, cessazione e variazione dei servizi e delle relative componenti;
- network monitoring e gestione degli apparati;
- supporto tecnico alla gestione dei malfunzionamenti;
- gestione centralizzata delle configurazioni e distribuzione del software;
- analisi delle prestazioni del servizio;
- rendicontazione;
- supporto alle amministrazioni nell'utilizzo dei servizi oggetto di Gara (formazione e consulenza).

La tabella seguente riepiloga le principali responsabilità del fornitore assegnatario e delle amministrazioni per l'erogazione dei servizi di sicurezza.

Responsabilità nell'erogazione dei servizi di sicurezza	
Fornitore assegnatario	**Amministrazione**

• Fornire una descrizione dettagliata del servizio che includa l'architettura, l'implementazione e le procedure di manutenzione evolutiva del sistema • Fornire, installare, configurare, gestire e manutenere, sia presso l'amministrazione che presso le proprie strutture, i dispositivi hardware/software necessari per l'erogazione del servizio • Monitorare il funzionamento del servizio al fine di determinare potenziali problemi e assicurare che vengano rispettati i livelli di servizio previsti (cfr. allegati 2c e 3a) • Prendere in carico i problemi connessi all'erogazione del servizio segnalati dall'utente al primo livello del proprio Call Center, incluse eventuali intrusioni/compromissioni inerenti al servizio • Interagire con altri fornitori SPC per la realizzazione del servizio VPN in modalità cooperativa • Gestire gli allarmi ed attivare le procedure di Incident Management • Gestire i malfunzionamenti delle componenti del servizio • Eseguire la manutenzione evolutiva del software per la componente che realizza il servizio • Mantenere in maniera evolutiva il piano degli indirizzi IP ed il piano di naming per la parte relativa al servizio offerto • Gestire l'anagrafico di rete relativamente ai collegamenti con sedi periferiche, enti esterni e/o altre strutture esterne • Effettuare il tuning delle configurazioni del servizio erogato • Effettuare il capacity planning del servizio erogato a fronte di necessità di aggiunte/modifiche • Informare l'amministrazione di eventuali situazioni che necessitano di interventi/decisioni da parte dell'amministrazione • Fornire report periodici all'amministrazione sullo stato, il livello di utilizzo, la disponibilità e le prestazioni del servizio offerto • Proporre all'amministrazione adeguamenti infrastrutturali • Fornire all'amministrazione l'accesso al proprio Centro di Gestione e Controllo per attività di monitoraggio passivo	• Definire i fabbisogni di sicurezza (incluse le politiche di sicurezza) • Mettere a disposizione del fornitore assegnatario i dispositivi hardware/software di proprietà utilizzati per l'implementazione e l'erogazione del servizio • Fornire la documentazione relativa alla topologia della rete, schemi di cablaggio e punti di accesso alla WAN/LAN • Fornire i requisiti e le informazioni di propria competenza per la configurazione del servizio • Segnalare anomalie di funzionamento o eventuali intrusioni/compromissioni • Adoperarsi affinché il fornitore assegnatario abbia visibilità almeno in lettura dei componenti di altri servizi gestiti da fornitori SPC qualora si ritenesse necessario per la corretta erogazione del servizio • Prendere in carico l'approvazione di adeguamenti proposti dal fornitore assegnatario • Intervenire/decidere sulle situazioni riferite dal fornitore assegnatario • Gestire gli allarmi provenienti da sistemi installati su dispositivi di proprietà (ad esempio, personal firewall) • Gestire le procedure di Incident Management

Tabella 26: Responsabilità del fornitore assegnatario e dell'amministrazione

Per l'espletamento di tali servizi il fornitore assegnatario dovrà dotarsi di un **Centro di Gestione per la sicurezza** (di seguito indicato con l'acronimo ***SOC, Security Operating Center***), che avrà il compito di gestire le risorse utilizzate per erogare i servizi di sicurezza.

2.12.1 Security Operating Center (SOC)

Il fornitore assegnatario dovrà realizzare un SOC, non necessariamente dedicato ai servizi SPC, che avrà il compito di gestire le risorse utilizzate per erogare i servizi di sicurezza.

Il SOC svolgerà anche i compiti della Unità Locale di Sicurezza SPC (cfr. allegato 2a), per la gestione degli aspetti relativi alla sicurezza. Il fornitore assegnatario dovrà nominare all'interno del SOC un **Responsabile Operativo della sicurezza** che dovrà coordinare l'Unità Locale di Sicurezza SPC e fungere da punto di contatto prioritario per tutte le problematiche di sicurezza che interessano i servizi SPC di sicurezza. Il Responsabile Operativo della sicurezza potrà avvalersi di sostituti i cui nominativi dovranno essere preventivamente comunicati all'amministrazione ed al CG-SPC.

Il SOC dovrà essere caratterizzato dalle seguenti funzionalità:

- **Progettazione e sviluppo dei servizi di sicurezza**: in relazione alle specifiche dei servizi disponibili agli utenti SPC, il SOC si occupa delle fasi di progetto e di sviluppo verificando in un ambiente di test presso la propria infrastruttura le funzionalità dei servizi. Ha la responsabilità di seguire gli aggiornamenti tecnologici sui sistemi proposti per assicurare le funzionalità erogate programmando con le amministrazioni ed il CG-SPC le modalità di patching e di migrazione.
- **Gestione e Monitoraggio**: il SOC, anche per il tramite di eventuali presidi territoriali, ha il compito di controllare e gestire in modo (semi)automatico e preventivo i dispositivi di rete e i sistemi impiegati per l'erogazione dei servizi forniti. Ha il compito di misurare i livelli di servizio.
- **Call Center** (cfr. paragrafo 2.12.2)*:* è il punto di contatto unificato per le richieste inviate al SOC, sia per i processi di provisioning (attivazione servizi, modifica policy, ecc.) sia per la gestione dei problemi e degli eventi di sicurezza. In relazione alla tipologia di richiesta il Call Center risolve la richiesta o coinvolge il Responsabile Operativo della sicurezza SPC presso il SOC. Il Call Center si occupa anche del processo di reporting relativi ai servizi offerti dal fornitore assegnatario.

Oltre alla struttura centralizzata del SOC il fornitore assegnatario, ove necessario e funzionale all'erogazione dei servizi, potrà dotarsi di presidi territoriali che erogano direttamente presso le amministrazioni le attività di gestione dei sistemi.

Il fornitore assegnatario dovrà garantire, all'interno del SOC o tra il SOC e punti esterni, i seguenti flussi di informazione:

- flusso tra il SOC del fornitore assegnatario ed il responsabile operativo del SOC di un fornitore SPC: rappresenta sia la segnalazione, in caso di escalation, di problemi sul servizio erogato in modalità cooperativa e su cui il fornitore SPC ha la competenza, sia le richieste/risposte di attivazione/(ri)configurazione/sospensione di servizi che richiedono l'intervento congiunto del SOC del fornitore SPC;
- flusso tra il SOC del fornitore assegnatario ed il CG-SPC; realizza lo scambio informativo relativo a:
  - la ricezione dal CG-SPC delle procedure operative e del materiale informativo per l'implementazione delle direttive emesse a garanzia del livello minimo di sicurezza del SPC;
  - le informazioni fornite al CG-SPC dal fornitore assegnatario durante una sessione di audit volta a verificare che il fornitore assegnatario rispetti il livello minimo di sicurezza imposto sul SPC;
  - lo scambio di informazioni (log, istruzioni di test e verifiche, contromisure, etc.) con il CG-SPC per la gestione, coordinata dal CERT SPC, degli incidenti informatici che coinvolgono il fornitore nell'ambito dei servizi erogati sul SPC e che impattano sul livello minimo di sicurezza imposto sul SPC;
- flusso tra il SOC del fornitore e l'Unità Locale di Sicurezza SPC dell'amministrazione; realizza lo scambio informativo relativo a:

- la ricezione dall'Unità Locale di Sicurezza SPC 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 fornitore assegnatario nell'ambito dei servizi erogati sul SPC e che impattano sul livello minimo di sicurezza imposto sul SPC, coordinata dal CERT SPC, o sul livello di sicurezza maggiore assicurato sul dominio dell'amministrazione;

- flusso tra il SOC del fornitore assegnatario e l'Unità Locale di Sicurezza SPC di un fornitore SPC; realizza lo scambio informativo relativo a:
  - informazioni (log, istruzioni di test e verifiche, contromisure, etc.) con l'Unità Locale di Sicurezza SPC presso il fornitore terzo per la gestione degli incidenti informatici che coinvolgono entrambi i fornitori nell'ambito dei servizi erogati sul SPC in modalità cooperativa e che impattano sul livello minimo di sicurezza imposto sul SPC, coordinata dal CERT SPC, o sul livello di sicurezza maggiore assicurato sul dominio dell'amministrazione;
- flusso tra il SOC del fornitore assegnatario ed il CERT SPC: rappresenta il flusso informativo che le due entità si scambiano per intraprendere le azioni necessarie all'analisi e alla gestione degli incidenti informatici e degli abusi che impattano sul livello minimo di sicurezza imposto sul SPC.

Attraverso il SOC, il fornitore assegnatario dovrà verificare in modo continuativo le prestazioni della propria infrastruttura di rete al fine di:

- gestire i sistemi utilizzati per l'erogazione dei servizi, con monitoraggio puntuale di ogni servizio;
- verificare il corretto dimensionamento complessivo dei sistemi;
- consentire una verifica dei livelli di servizio contrattualmente stabiliti ed il calcolo di statistiche (cfr. allegati 2c e 3a);
- fornire reportistica.

Il SOC dovrà inoltre includere una Base Dati contenente informazioni su:

- ubicazione, tipologia e configurazione dei sistemi utilizzati;
- policy configurate per ciascun sistema;
- elenco dei responsabili dei sistemi;
- misurazioni dei livelli di servizio che includono almeno i dati oggetto di tutti i report periodici previsti negli allegati 2c e 3a;
- log delle richieste di intervento pervenute al Call Center;
- log dei trouble ticket;
- classificazione dei guasti a seconda dei livelli di servizio contrattualizzati
- dati di riscontro della qualità.

La Base Dati dovrà essere interamente accessibile in lettura da parte dell'amministrazione mediante Web Browser. Il fornitore assegnatario dovrà a tal fine fornire le credenziali di accesso (username e password secondo le policy definite per il SPC) per la consultazione della Base Dati e per l'esportazione dei dati. In particolare dovranno essere assicurate alle singole amministrazioni le seguenti funzionalità:

- consultazione diretta della Base Dati relativa alla risorse di sicurezza di propria competenza tramite interfaccia grafica che consenta la generazione guidata di report, grafici, e query complesse;
- funzionalità di esportazione dei dati, secondo formati standard, contenuti nella porzione di Base Dati relativa alla risorse di rete di propria competenza.

Il fornitore assegnatario dovrà, qualora l'amministrazione ne faccia richiesta, rendere disponibile una stazione dedicata al monitoraggio degli apparati utilizzati e per la consultazione dei log generati dagli stessi apparati. La stazione di monitoraggio dovrà consentire una visione integrata e con report unificato di tutti i dispositivi installati per il particolare servizio offerto.

Il SOC dovrà acquisire dalla sorgente ufficiale il "Tempo Ufficiale della Rete" situate presso il NOC-QXN (cfr. paragrafo 6.3.3) utilizzarlo come riferimento ai fini della marcatura con "time stamp" dei log e dei TT, nonché per tutte le altre funzioni di gestione della rete che richiedono un riferimento temporale.

Su richiesta dell'amministrazione o del CNIPA, il fornitore assegnatario dovrà, secondo procedure concordate, consentire l'accesso al SOC al personale incaricato del CG-SPC per effettuare verifiche sulle modalità di espletamento del servizio.

2.12.2 Call Center

Anche per i servizi di sicurezza l'amministrazione dovrà poter accedere ai servizi di Call Center descritti nel paragrafo 1.5.3 .

2.12.3 Servizi di Fault Management

Il call center del fornitore assegnatario dovrà erogare, anche per i servizi di sicurezza, i servizi di Fault Management in maniera analoga a quanto descritto nel paragrafo 1.5.4 .

In particolare i sistemi di Trouble Ticketing utilizzati per l'erogazione dei servizi di connettività e di sicurezza dovranno essere integrati.

2.12.4 Servizi di Provisioning, Configuration e Change Management

Il fornitore assegnatario dovrà erogare le seguenti prestazioni:

- attivazione/cessazione di nuovi servizi di sicurezza e delle relative componenti;
- trasloco dei servizi di sicurezza;
- variazione delle componenti dei servizi di sicurezza;
- variazione delle policy e delle configurazioni di sicurezza adottate;

- attuazione degli adeguamenti, riconfigurazioni o ristrutturazioni richiesti da attività di“system tuning”;
- caricamento ed attivazione di nuove release software su tutti i sistemi utilizzati per l’erogazione del servizio.

Il fornitore assegnatario dovrà gestire e controllare tutte le configurazioni hardware e software degli apparati utilizzati per l'erogazione dei servizi, mantenendo aggiornato un database delle configurazioni (integrato con le Basi Dati di NOC e SOC) che consenta:

- l’inventario delle configurazioni hardware e software e delle personalizzazioni necessarie in modo da facilitare le operazioni di ripartenza e riallineamento a fronte di un qualsiasi problema legato alle funzionalità dei sistemi gestiti;
- la pianificazione delle attività di gestione e di aggiornamento dei sistemi.

2.12.5 Servizi di Rendicontazione

Il fornitore assegnatario dovrà erogare, anche per i servizi di sicurezza, i servizi di Rendicontazione in maniera analoga a quanto descritto nel paragrafo 1.5.6 .

2.12.6 Servizi di Supporto sistemistico

Il fornitore assegnatario dovrà erogare alle amministrazioni il supporto necessario per la redazione del “Piano dei fabbisogni dell’amministrazione” (cfr. paragrafo 4.1) propedeutico alla definizione dei contratti esecutivi. Tale supporto dovrà consentire alle amministrazioni di valutare le opportunità offerte dai servizi SPC e di analizzare gli impatti tecnici ed organizzativi in relazione all'infrastruttura di rete pre-esistente presso la singola amministrazione.

All’avvio delle attività il fornitore assegnatario dovrà supportare l’amministrazione nella scelta dei servizi da contrattualizzare e nella realizzazione di un’analisi preliminare volta ad evidenziare eventuali criticità nell’architettura di rete e nelle componenti tecnologiche presenti nel sistema informativo dell’amministrazione. Oltre ai servizi proposti, lo studio di fattibilità dovrà riportare i tempi di realizzazione e l’evidenza d’oneri aggiuntivi a carico dell’amministrazione necessari alla fruizione dei servizi (ad esempio, predisposizione degli spazi, adeguamento alimentazione elettrica, aggiornamento di release software, etc).

2.12.7 Consulenza sui servizi e sistemi di sicurezza

Il fornitore assegnatario dovrà erogare un servizio di Consulenza sui servizi e sistemi di sicurezza comprendente:

- progettazione del sistema di sicurezza del Sistema Informativo;
- supporto decisionale all'adozione di standard e tecnologie volte alla messa in sicurezza del Sistema Informativo;
- stesura di un piano di sicurezza: attività di consulenza che prevede la classificazione dei beni da proteggere e l'analisi dei rischi per elaborare un piano per la sicurezza chiaro e preciso. Il piano di sicurezza deve consentire all’amministrazione di mettersi in regola con gli adempimenti in materia di privacy e sicurezza dei dati sensibili ai sensi del D. L. 196/2003;

- consulenza per la pianificazione e lo sviluppo di infrastrutture a chiave pubblica (Public Key Infrastructure, PKI). Il fornitore assegnatario dovrà provvedre a:
    - progettazione della PKI per l'amministrazione;
    - installazione e messa in opera di Certification Authority e Registration Authority;
    - sviluppo di applicazioni integrate nella PKI;
- consulenza sulle modalità d'integrazione della PKI dell'amministrazione con la PKI del SPC;
- supporto legale alle problematiche di gestione dei dati sensibili ed alla sicurezza della detenzione degli stessi;
- supporto legale per la gestione degli incidenti informatici;
- consulenza e seminari su standard PKCS, ISO9594, ITU.T X.509, RFC PKIX, ASN.1 e regolamenti tecnici CNIPA.

I report sul servizio dipendono dalla particolare attività consulenziale richiesta e saranno esplicitati dall'amministrazione in fase di stipula del contratto esecutivo (cfr. allegati 2e e 3b).

2.12.8 Formazione

Il fornitore assegnatario dovrà erogare alle amministrazioni servizi di formazione. Le attività di formazione potranno essere svolte, a discrezione della amministrazione, e previo accordo tra quest'ultima ed il fornitore assegnatario:

- presso una sede centrale (modalità centralizzata) realizzata e attrezzata a carico del fornitore assegnatario presso una propria sede;
- presso i locali dell'amministrazione interessata (formazione decentrata); tutti gli oneri per l'allestimento delle sale attrezzate decentrate saranno a carico del fornitore assegnatario.

Il fornitore assegnatario dovrà redigere un Documento intitolato **"Piano di dettaglio di formazione"** (cfr. paragrafo 8.2) per singola amministrazione. Al suddetto piano dovranno essere allegati i curricula dei docenti.

Servizi di formazione di base

Il fornitore assegnatario dovrà erogare servizi di formazione di base per le figure professionali che svolgono presso l'amministrazione un ruolo operativo di supervisione della rete e di help desk di primo livello per gli utenti.

I suddetti servizi dovranno tener conto delle necessità e delle conoscenze possedute dai destinatari delle attività di formazione e trattare argomenti che permettano di comprendere l'erogazione dei servizi SPC, l'organizzazione della QXN, la configurazione e l'esercizio della rete, le funzionalità offerte dalla stazione di supervisione, le problematiche di garanzia della qualità del servizio, le modalità di ripristino della funzionalità della rete oltre che una conoscenza di base di networking che comprenda almeno:

- protocollo IP;
- principali protocolli di trasporto (TCP, UDP) ed applicativi (FTP, HTTP, Telnet, etc.);
- principali architetture di rete in ambito locale (LAN) e geografiche (WAN);

- descrizione dei principali rischi di sicurezza;
- strumenti di crittografia;
- descrizione funzionale dei principali apparati di sicurezza (firewall, antivirus, IDS, etc.);
- introduzione alle VLAN e al protocollo IPSec.

I corsi di formazione saranno realizzati a classi che prevedano un numero di discenti pari a:

- 3-5 discenti per le amministrazioni con un numero di accessi superiore alle 15 unità;
- 1-3 discenti per amministrazioni con un numero di accessi non superiore alle 15 unità.

La durata dei corsi sarà concordata con l'amministrazione sulla base del programma formativo e sulla base del grado di conoscenza dei discenti ma non potrà superare i 3 gg lavorativi.

Il servizio di formazione dovrà essere svolto da personale qualificato, in possesso di almeno una certificazione in ambito networking e sicurezza.

Servizi di formazione specifici

Il fornitore assegnatario dovrà presentare, su richiesta dell'amministrazione, un progetto di formazione specifico per le risorse dell'amministrazione.

Gli argomenti dei corsi di formazione riguarderanno tematiche relative alle reti di telecomunicazione a alla sicurezza dei Sistemi Informativi, tra cui:

- formazione sulla normativa vigente in termini di sicurezza informatica;
- metodologie per la definizione e gestione della politica di sicurezza aziendale;
- analisi di tecnologie a supporto della sicurezza informatica;
- metodologie e strumenti per la gestione del rischio;
- metodologie e strumenti per la gestione degli incidenti informatici;
- crittografia ed infrastrutture a chiave pubblica e privata (PKI).

Il fornitore assegnatario dovrà redigere un Documento intitolato **"Piano di dettaglio di formazione"** (cfr. paragrafo 8.2) entro 3 mesi dalla sottoscrizione del contratto esecutivo con la singola amministrazione. Al suddetto piano dovranno essere allegati i curriculum vitae dei docenti. I docenti dovranno essere in possesso di almeno una o più certificazioni in ambito networking e sicurezza e di un'esperienza nella formazione di almeno 3 anni.

I corsi di formazione saranno realizzati a classi che prevedano un minimo di 5 discenti ed un massimo di 10. Il numero delle sessioni e, conseguentemente, la durata dei corsi sarà concordata con l'amministrazione sulla base del programma formativo e sulla base del grado di conoscenza dei discenti.

3 SERVIZI OPA E SERVIZI OPO

Come indicato nella Lettera d'invito i fornitori dovranno presentare due differenti tipologie di offerta:

- un'**Offerta Per le Amministrazioni (OPA)**;
- un'**Offerta Per gli altri Operatori del SPC (OPO) da parte del fornitore aggiudicatario**, riservata agli altri fornitori assegnatari che ne facciano richiesta, contenente servizi corrispondenti ad alcuni servizi di connettività OPA con specifici livelli di servizio. L'OPO non potrà comunque essere utilizzata ai fini dell'erogazione di servizi a clienti esterni al SPC.

Il fornitore assegnatario sarà comunque responsabile in toto dell'erogazione dei servizi all'amministrazione a prescindere che tali servizi siano erogati utilizzando o meno l'offerta OPO del fornitore aggiudicatario. Pertanto il fornitore assegnatario costituirà l'interfaccia unica con l'amministrazione per quanto riguarda la fornitura dei servizi, la gestione, il call center, il fault management e la rendicontazione (avvalendosi eventualmente dei corrispondenti servizi OPO).

La tabella seguente elenca la composizione, in termini dei servizi precedentemente descritti, delle offerte OPO e OPA:

	Servizio	Rif. Capitolato Tecnico	OPA	OPO
Trasporto	Always-on	§ 1.1.1	√	√
	Dial-up	§ 1.1.2	√	√
	Wireless	§ 1.1.3	√	√
Supporto	Gestione degli indirizzi pubblici	§ 1.2.1	√	√
	DNS	§ 1.2.2	√	√
VoIP	VoIP	§ 1.3	√	√
Interoperabilità di base	Posta elettronica	§ 1.4.1	√	√
	Trasporto di protocolli proprietari	§ 1.4.2	√	
	Servizi di Data Center	§ 1.4.3	√	

Manutenzione e assistenza dei servizi di connettività	NOC	§ 1.5.1	√	√
	Call Center	§ 1.5.3	√	√
	Fault Management	§ 1.5.4	√	√
	Provisioning, Configuration e Change Management	§ 1.5.5	√	√
	Rendicontazione	§ 1.5.6	√	√
	Supporto sistemistico	§ 1.5.7	√	√
	Formazione	§ 1.5.8	√	√
Sicurezza	Firewall management	§ 2.3	√	
	Antivirus & content filtering management	§ 2.4	√	
	NIDS management	§ 2.5	√	
	Event & Log Monitoring management	§ 2.6	√	
	VPN management	§ 2.7	√	
	Hardening dei sistemi	§ 2.8	√	
	NAT management	§ 2.9	√	
	HIDS management	§ 2.10	√	

	Vulnerability assessment	§ 2.11	√	
Manutenzione e assistenza dei servizi di sicurezza	SOC	§ 2.12.1	√	
	Call Center	§ 2.12.2	√	
	Fault Management	§ 2.12.3	√	
	Provisioning, Configuration e Change Management	§ 2.12.4	√	
	Rendicontazione	§ 2.12.5	√	
	Supporto sistemistico	§ 2.12.6	√	
	Consulenza sui servizi e sistemi di sicurezza	§ 2.12.7	√	
	Formazione	§ 2.12.8	√	

Tabella 27: Servizi OPA e servizi OPO

Il fornitore aggiudicatario dovrà erogare in OPO i servizi di supporto e di manutenzione e assistenza di connettività soltanto congiuntamente all'erogazione di servizi di trasporto, VoIP ed interoperabilità di base.

4 MODALITA' DI ATTIVAZIONE DEI SERVIZI

Il fornitore assegnatario dovrà effettuare tutte le attività descritte nei paragrafi successivi sia nel caso della migrazione di un'amministrazione da servizi preesistenti sia nel caso di realizzazioni ex novo.

Nel caso in cui l'amministrazione fruisca di servizi preesistenti, il fornitore assegnatario dovrà esplicitamente prevedere, congiuntamente con l'amministrazione contraente, le procedure di attivazione che permettano il mantenimento dell'operatività durante le fasi di migrazione.

4.1 Condivisione delle informazioni

L'amministrazione allegherà al Contratto esecutivo OPA un documento intitolato **"Piano dei fabbisogni"**, contenente le indicazioni sul tipo, le quantità ed il dimensionamento dei servizi richiesti.

Il fornitore assegnatario dovrà impegnarsi a supportare l'amministrazione nella redazione del Piano dei fabbisogni.

Il fornitore assegnatario avrà facoltà di condurre, con proprio personale tecnico o altro personale da lui stesso incaricato, e congiuntamente con i referenti dell'amministrazione interessata, sopralluoghi su 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).

A tale scopo l'amministrazione dovrà consentire l'accesso del personale del fornitore assegnatario, o di personale specialistico dallo stesso incaricato, ai locali tecnici in cui saranno installati gli apparati e la presenza ed assistenza del personale tecnico della sede interessata.

Il fornitore assegnatario dovrà approntare il calendario dei sopralluoghi necessari. Tale calendario dovrà indicare, per ciascuna sede oggetto di sopralluogo, il nominativo dell'incaricato dal fornitore assegnatario per il sopralluogo, con gli estremi di un documento di riconoscimento e l'elenco delle verifiche da effettuare. Il calendario sarà sottoposto all'approvazione dell'amministrazione interessata.

4.2 Progetto dei fabbisogni

Il fornitore assegnatario, nel rispetto delle modalità indicate nell'allegato 2, dovrà consegnare all'amministrazione un documento intitolato **"Progetto dei fabbisogni"** (cfr. paragrafo 8.2.2), nel quale raccoglierà le richieste dell'amministrazione contenute nel Piano dei fabbisogni e formulerà una proposta tecnico/economica (secondo le condizioni oggetto della presente gara).

Il Progetto dei fabbisogni dovrà contenere inoltre i seguenti allegati (cfr. paragrafo 8.2.2):

- **Costi** previsti per la realizzazione del progetto, ottenuti applicando ai servizi richiesti i prezzi unitari di cui all'allegato 2d;
- **Modalità di presentazione e approvazione degli Stati di Avanzamento Mensili**.
- **Piano di Attuazione**, con l'indicazione dei tempi di realizzazione del suddetto progetto, articolato nei seguenti allegati:
    - **Documento programmatico di gestione della sicurezza dell'amministrazione**;

- **Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi**.

Il Progetto dei Fabbisogni potrà essere modificato e/o aggiornato dall'amministrazione ogni qualvolta questa lo ritenga necessario.

4.2.1 Project Management

Il fornitore assegnatario dovrà erogare un servizio di project management consistente nella pianificazione, gestione e verifica delle attività mirate al completamento del progetto. La definizione delle attività sarà responsabilità di un gruppo di lavoro costituito almeno da:

- responsabile del progetto presso la singola amministrazione;
- project manager del fornitore assegnatario.

4.3 Site preparation

Il fornitore assegnatario dovrà definire all'interno del Piano di Attuazione (nell'allegato Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi) le specifiche riguardanti la predisposizione dei siti.

L'organizzazione e la realizzazione delle attività saranno a cura dell'amministrazione.

Sarà peraltro cura dell'amministrazione informare tempestivamente il fornitore assegnatario di variazioni delle attività suddette che possano influenzare lo svolgimento del piano di installazione (cfr. paragrafo 4.4).

4.4 Installazione

Il fornitore assegnatario dovrà definire, congiuntamente con l'amministrazione, il piano di installazione dei servizi. Il piano di installazione dovrà rispettare i seguenti requisiti minimi:

- gli interventi dovranno essere effettuati in intervalli orari definiti dall'amministrazione coerentemente con le proprie esigenze di operatività;
- l'operatività del servizio dovrà 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 dovrà essere minimo.

Qualora un'operazione di installazione dovesse costituire causa di disservizio, il fornitore assegnatario dovrà adoperarsi per garantire un ripristino immediato della condizione preesistente.

A partire dalla data di decorrenza del contratto esecutivo il fornitore assegnatario dovrà procedere al installazione delle sedi secondo le modalità temporali previste dal Piano di attuazione (cfr. paragrafo 4.2). In fase di configurazione delle TdR per ogni sede individuata il fornitore assegnatario, congiuntamente con l'amministrazione, dovrà:

- contattare il referente tecnico della sede;
- concordare le modalità ed i tempi di interventi on-site;
- effettuare una verifica del sito, se necessaria;

- procedere all’attestazione del collegamento;
- partecipare alle attività di test ed emettere un verbale per collaudo eseguito con esito positivo.

4.5 Migrazione

Il fornitore assegnatario dovrà considerare prioritaria, sia nella pianificazione che nell’esecuzione dell’attivazione, la salvaguardia dell’operatività delle amministrazioni nel periodo di tempo durante il quale avverrà la migrazione dai servizi attuali ai servizi SPC.

In particolare, nel caso in cui un’operazione di attivazione del servizio dovesse costituire causa di malfunzionamento, il fornitore assegnatario dovrà assicurare la possibilità di un ripristino immediato della condizione preesistente.

L’amministrazione concorderà con i fornitori uscenti la loro partecipazione alle attività che ne richiedono l’intervento.

5 INTERFACCIA CON IL CG-SPC

Il fornitore assegnatario dovrà interfacciare i propri sistemi informativi con quelli del CG-SPC per fornire, almeno giornalmente, i dati relativi ai parametri di QoS, di fault, di provisioning ed informazioni di configurazione. Il fornitore assegnatario dovrà quindi garantire la piena disponibilità ad uniformarsi alle modalità di scambio emesse dal CNIPA sentiti il CG-SPC ed i fornitori assegnatari; in ogni caso tale scambio si baserà su file formattati secondo il linguaggio XML. Le modalità di invio di tali file saranno basate su protocolli standard (mail, FTP, etc.) che potranno includere meccanismi di protezione di dati confidenziali (IPSEC, SSL, SSH).

Il fornitore assegnatario dovrà garantire la piena disponibilità ad implementare un meccanismo di scambio dati tra le diverse entità interessate, che coinvolga almeno tutte le informazioni di seguito riportate. Il fornitore assegnatario dovrà inoltre garantire la disponibilità ad ampliare il set di informazioni scambiate, qualora tale necessità si dovesse successivamente manifestare.

5.1 Dati Prestazionali

Vengono riportate di seguito le informazioni minime che il fornitore assegnatario dovrà rendere disponibili al CG-SPC:

- **Round Trip Delay (RTD).** Ogni campione di misura relativo al RTD dovrà contenere almeno le seguenti informazioni:
  - Identificativo del fornitore assegnatario
  - Identificativo dell'amministrazione
  - Identificativo della misura
  - Identificativo della CdS
  - Istante di campionamento
  - Identificativo del primo PAS (origine)
  - Identificativo del secondo PAS (destinazione)
  - Il valore della misura espresso in millisecondi
- **One Way Delay.** Ogni campione di misura relativo al OWD dovrà contenere almeno le seguenti informazioni:
  - Identificativo del fornitore assegnatario
  - Identificativo dell'amministrazione
  - Identificativo della misura
  - Identificativo della CdS
  - Istante di campionamento
  - Identificativo del primo PAS (origine)
  - Identificativo del secondo PAS (destinazione)
  - Il valore della misura espresso in millisecondi

- **Packet Loss.** Ogni campione di misura relativo alla perdita di pacchetti dovrà contenere almeno le seguenti informazioni:
    - Identificativo del fornitore assegnatario
    - Identificativo dell'amministrazione
    - Identificativo della misura
    - Identificativo della CdS
    - Istante di campionamento
    - Identificativo del primo PAS (origine)
    - Identificativo del secondo PAS (destinazione)
    - Il valore della misura relativo alla tratta origine-destinazione, espresso in percentuale
    - Il valore della misura relativo alla tratta destinazione-origine, espresso in percentuale
- **Jitter.** Ogni campione di misura relativo al jitter dovrà contenere almeno le seguenti informazioni:
    - Identificativo del fornitore assegnatario
    - Identificativo dell'amministrazione
    - Identificativo della misura
    - Identificativo della CdS
    - Istante di campionamento
    - Identificativo del primo PAS (origine)
    - Identificativo del secondo PAS (destinazione)
    - Il valore della misura relativo alla tratta origine-destinazione del massimo positivo, espresso in millisecondi
    - Il valore della misura relativo alla tratta origine-destinazione del minimo negativo, espresso in millisecondi
    - Il valore della misura relativo alla tratta destinazione-origine del massimo positivo, espresso in millisecondi
    - Il valore della misura relativo alla tratta destinazione-origine del minimo negativo, espresso in millisecondi
- **Banda Utilizzata.** Ogni campione di misura relativo alla banda utilizzata dovrà contenere almeno le seguenti informazioni:
    - Identificativo del fornitore assegnatario
    - Identificativo dell'amministrazione
    - Identificativo della misura
    - Istante di campionamento
    - Identificativo del PAS

- Il valore della misura relativa alla banda in upstream espresso in Kb/s
- Il valore della misura relativa alla banda in downstream espresso in Kb/s

Oltre ai parametri di QoS di rete, il fornitore assegnatario dovrà consegnare al CG-SPC i dati relativi alle performance dei servizi di DNS e posta elettronica.

- **Ritardo di risposta del servizio DNS.** Ogni campione di misura relativo al ritardo di risposta per il servizio di DNS dovrà contenere almeno le seguenti informazioni:
  - Identificativo del fornitore assegnatario
  - Identificativo dell'amministrazione
  - Identificativo della misura
  - Istante di campionamento
  - Identificativo del server DNS
  - Il valore della misura espresso in millisecondi
- **Ritardo di risposta del servizio di posta elettronica.** Ogni campione di misura relativo al ritardo di risposta per il servizio di posta elettronica dovrà contenere almeno le seguenti informazioni:
  - Identificativo del fornitore assegnatario
  - Identificativo dell'amministrazione
  - Identificativo della misura
  - Istante di campionamento
  - Identificativo del mail server
  - Il valore della misura espresso in secondi
- **Throughput del servizio di posta elettronica.** Ogni campione di misura relativo al throughput del servizio di posta elettronica dovrà contenere almeno le seguenti informazioni:
  - Identificativo del fornitore assegnatario
  - Identificativo dell'amministrazione
  - Identificativo della misura
  - Periodo di osservazione
  - Identificativo del mail server
  - Il valore della misura espresso in Mb/s

5.2 Dati di Affidabilità

Il fornitore assegnatario dovrà consegnare al CG-SPC almeno le informazioni riportate di seguito:

- **Disponibilità.** Ogni campione di misura relativo alla disponibilità di un PAS dovrà contenere almeno le seguenti informazioni:
    - Identificativo del fornitore assegnatario
    - Identificativo dell'amministrazione
    - Identificativo della misura
    - Tempo di osservazione
    - Identificativo del PAS
    - La misura effettuata misurata in percentuale
- **Tempo di Ripristino.** Ogni campione di misura relativo al tempo di ripristino di un disservizio relativo ad un PAS dovrà contenere almeno le seguenti informazioni:
    - Identificativo del fornitore assegnatario
    - Identificativo dell'amministrazione
    - Identificativo della misura
    - Identificativo della CdS (se applicabile)
    - Identificativo del tipo di disservizio
    - Istante di inizio del disservizio
    - Identificativo del PAS
    - La misura effettuata misurata espressa in ore
- **Ripetitività dei disservizi.** Ogni campione di misura relativo alla ripetitività dei disservizi relativi ad un PAS dovrà contenere almeno le seguenti informazioni:
    - Identificativo del fornitore assegnatario
    - Identificativo dell'amministrazione
    - Identificativo della misura
    - Identificativo della CdS (se applicabile)
    - Identificativo del tipo di disservizio
    - Tempo di osservazione
    - Identificativo del PAS
    - Numero dei disservizi
- **Dati di call center/Fault management.** Ogni campione di misura relativo all'attività del call center dovrà contenere almeno le seguenti informazioni:
    - Identificativo del fornitore assegnatario
    - Identificativo dell'amministrazione
    - Identificativo del TT
    - Tempo di risposta dell call center

- Identificativo del PAS
- Numero dei disservizi

5.3 Dati di Provisioning

Il fornitore assegnatario dovrà consegnare al CG-SPC le informazioni minime riportate di seguito:

- **Tempo di provisioning di un nuovo servizio di trasporto**: tempo, misurato in giorni solari, intercorso tra la richiesta dell'amministrazione e la disponibilità di un nuovo servizio.
- **Tempo di provisioning di una nuova componente**: tempo, misurato in giorni solari, intercorso tra la richiesta dell'amministrazione e la variazione e/o aggiunta di una nuova componente di accesso e/o di trasferimento per un accesso già esistente.
- **Tempo di provisioning di un trasloco interno**: tempo, misurato in giorni solari, intercorso tra la richiesta dell'amministrazione e la disponibilità del servizio presso un nuovo punto di attestazione indicato dall'amministrazione all'interno dello stesso sito.
- **Tempo di provisioning di un trasloco esterno**: tempo, misurato in giorni solari, intercorso tra la richiesta dell'amministrazione e la disponibilità del servizio presso un nuovo punto di attestazione indicato dall'amministrazione presso un diverso sito.

5.4 Log

Il fornitore assegnatario dovrà garantire l'invio dei log relativi agli incidenti di sicurezza verificatisi nel SPC. Il CG-SPC, qualora lo ritenga opportuno, potrà richiedere al NOC/SOC del fornitore assegnatario l'abilitazione di un livello di logging appropriato ed invio dei log relativi al fine di eseguire controlli e verifiche sullo stato della rete.

SEZIONE II – SERVIZI EROGATI DALLA SOCIETA' CONSORTILE

6 QUALIFIED EXCHANGE NETWORK (QXN)

I fornitori assegnatari dovranno realizzare, attraverso una **Società Consortile (SC-QXN)** (cfr. allegato 4) alla quale potranno partecipare tutti i fornitori di connettività SPC[2], una rete di interconnessione tra le reti di tutti i fornitori di connettività SPC denominata Qualified eXchange Network (QXN). La società consortile dovrà garantire lo svolgimento di tutte le attività di:

- progettazione iniziale della QXN;
- realizzazione della QXN;
- definizione delle modalità di collaudo;
- gestione della QXN;
- stesura delle convenzioni di adesione ai servizi;
- erogazione dei servizi della QXN ai soggetti collegati;
- progettazione evolutiva, a fronte di nuove esigenze e/o di evoluzione tecnologica, della QXN.

Una volta costituita la SC-QXN dovrà descrivere tali attività all'interno di documenti da redigere secondo le modalità ed i contenuti indicati nel paragrafo 8.1 ; tale documentazione dovrà essere approvato dal CNIPA.

6.1 Caratteristiche della QXN

La rete di interconnessione avrà caratteristiche e compiti simili a quelli di un Internet eXchange Point. La struttura della QXN dovrà pertanto possedere le seguenti caratteristiche:

- architettura geograficamente distribuita con almeno due nodi connessi tra loro con link ridondati di capacità almeno pari a 34 Mb/s e comunque adeguata alla quantità di traffico trasportato;
- nodi dell'infrastruttura co-locati presso NAP pubblici già esistenti per garantire la migliore possibilità di partecipazione al SPC dei fornitori di servizi di connettività;
- nodi in grado di effettuare il routing di pacchetti IP al fine di garantire il corretto flusso di traffico attraverso l'infrastruttura;
- nodi e collegamenti dimensionati in modo da garantire il rispetto delle caratteristiche di qualità del SPC.

[2] Con fornitore SPC si intendono tutti i fornitori assegnatari e tutti gli operatori iscritti negli elenchi di cui all'art. 11 del d.lgs. 42/2005 che abbiano aderito alle norme contrattuali e tecniche del SPC contrattualizzando una amministrazione pubblica.

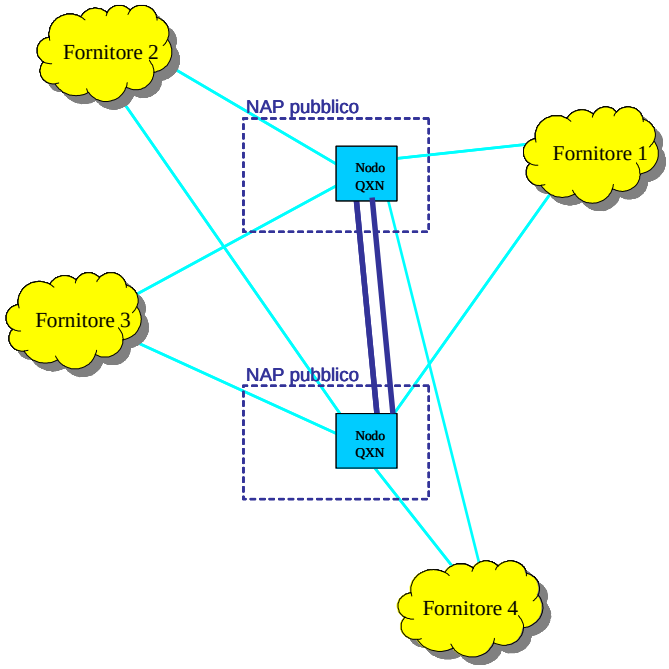

Figura 11, Architettura della QXN

I fornitori assegnatari dovranno connettersi alla QXN attraverso collegamenti ad almeno due nodi della QXN. In ciascuno dei nodi su cui soi connette il fornitore assegnatario dovrà installare a suo carico almeno due Border Router (BR), su cui sarà convogliato tutto il traffico proveniente dal SPC da e per le amministrazioni attestate sulla propria rete.

Il traffico non dovrà attraversare la QXN (anche limitatamente alle componenti LAN esterne all'AS della QXN, ma di sua competenza) qualora si tratti di:

- traffico Intranet o Infranet tra sedi collegate alla rete dello stesso fornitore assegnatario (connessioni di tipo A1 nella Figura 12);
- traffico che coinvolge un'amministrazione ed un soggetto non collegato al SPC (connessioni di tipo A2);
- traffico tra soggetti non collegati al SPC.

Viceversa il traffico dovrà transitare sui nodi della QXN ogni qualvolta le amministrazioni coinvolte nello scambio di traffico siano connesse alle reti di due fornitori assegnatari differenti (connessione di tipo B in Figura 12).

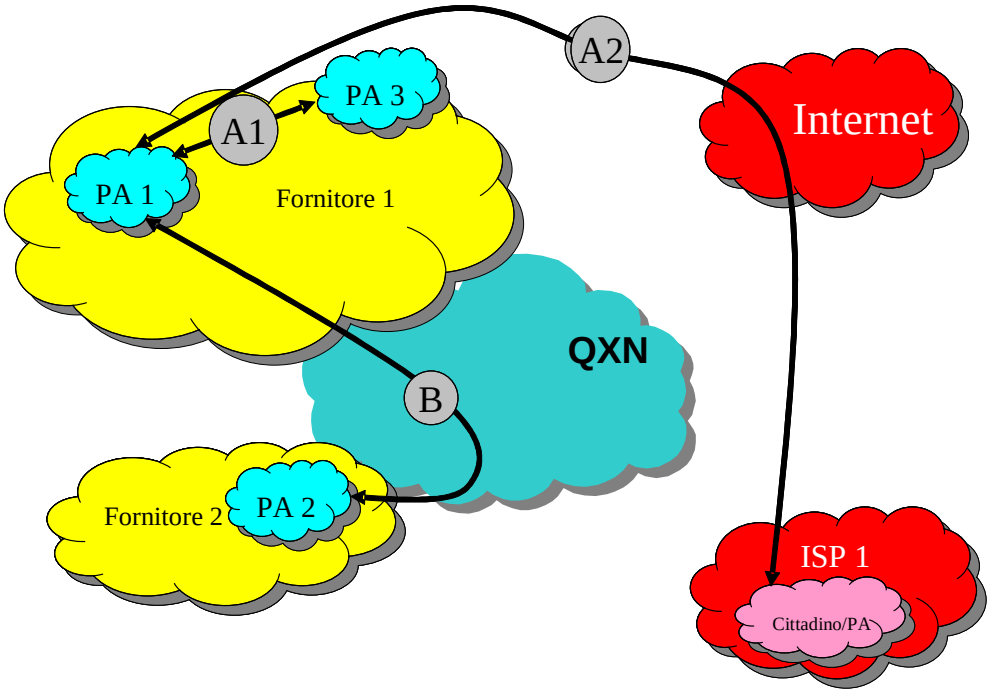

Figura 12, Traffico sulla QXN

6.2 Servizi erogati dalla QXN

La QXN dovrà erogare servizi di:

- **Housing**: consistente nella locazione di spazio per alloggiare gli apparati dei fornitori SPC all'interno di una struttura in grado di offrire elevati standard qualitativi in termini di sicurezza fisica degli ambienti (cfr paragrafo 6.6.1). Il servizio di housing dovrà garantire:
  - alimentazione;
  - condizionamento;
  - vigilanza;
  - logistica;
  - pulizia.
- **Accesso**: fornitura di porte Gigabit Ethernet per la connessione degli apparati di accesso dei fornitori SPC alla LAN interna dei nodi della QXN.
- **Banda**: fornitura di servizi di banda garantita in accesso all'infrastruttura della QXN, nonché il trasporto di pacchetti IP attraverso l'infrastruttura della QXN.
- **Tempo ufficiale di rete**: servizio di sorgente del tempo ufficiale di rete per permettere la sincronizzazione del tempo a tutti i fornitori e alle amministrazioni che ne facciano richiesta.

Per quanto riguarda le prestazioni, la progettazione della QXN dovrà rispettare i seguenti valori minimi prestazionali:

PARAMETRO	SLA

Disponibilità del singolo servizio	99,99%
Tempo di attraversamento dei pacchetti (OWD)	20 ms
Tasso di perdita dei pacchetti	0,05%

Tabella 28: Valori minimi prestazionali della QXN

6.3 Organizzazione della SC-QXN

I fornitori assegnatari costituenti la SC-QXN dovranno realizzare una struttura organizzativa per la gestione tecnica della QXN che prevede almeno le seguenti strutture:

- Direzione Tecnica affidata alla responsabilità di un Direttore tecnico;
- Comitato Tecnico;
- Unità responsabile della Sicurezza;
- Network Operations Center (NOC-QXN).

La SC-QXN dovrà redigere e mantenere aggiornato un documento intitolato **"Documento di Organizzazione della SC-QXN"** (cfr. paragrafo 8.1) che illustrerà in dettaglio le unità funzionali/organizzative adottate ed i rapporti intercorrenti fra di esse.

6.3.1 Direzione Tecnica

Il Direttore Tecnico avrà il compito di coordinare tutte le attività della Direzione Tecnica della SC-QXN. Il Direttore Tecnico avrà la facoltà di convocare il Comitato Tecnico e di sottoporre le delibere da questo emanate al Consiglio di Amministrazione.

Il Direttore Tecnico avrà anche la responsabilità di garantire l'operatività della QXN e di supervedere le attività del NOC-QXN (cfr. paragrafo 6.3.3).

6.3.2 Comitato Tecnico

Il Direttore Tecnico, nelle sue decisioni, è tenuto a valersi degli indirizzi e suggerimenti di un **Comitato Tecnico.**

Fanno parte del Comitato Tecnico:

- il Direttore tecnico della Società;
- un rappresentante per ogni socio della Società che detenga almeno il 5% del Capitale Sociale;
- un rappresentante del CNIPA;
- un rappresentante del CG-SPC;

- il Direttore tecnico di ogni NAP in cui siano co-locati i nodi della QXN.

I compiti del Comitato Tecnico dovranno includere le seguenti attività:

- definizione delle caratteristiche tecniche della QXN e dei requisiti tecnici di interfaccia per il collegamento delle reti dei fornitori SPC alla stessa;
- azioni e consulenza nei confronti della Commissione di coordinamento SPC per la definizione di regole tecniche condivise per il funzionamento del SPC (ad esempio politiche di indirizzamento, regole congiunte di marchiatura del traffico per il rispetto del qualità di servizio);
- verifica periodica dei livelli di servizio e della qualità dello stesso sia per gli aspetti di infrastruttura interna della QXN sia per i singoli collegamenti dei partecipanti;
- intervento nei casi in cui gravi malfunzionamenti o errori di configurazione su apparecchiature di un fornitore SPC pregiudichino il buon funzionamento della QXN o di parte di essa;
- promozione di iniziative atte a migliorare i servizi offerti.

6.3.3 Network Operations Center della QXN (NOC-QXN)

La SC-QXN dovrà allestire e gestire il **Network Operations Center della QXN (NOC-QXN)** per assicurare tutte le funzionalità di gestione della QXN. Il NOC-QXN dovrà rispettare tutti i requisiti minimi indicati nel presente paragrafo.

Requisiti generali

Il NOC-QXN dovrà essere operativo H24. Le funzioni generali che il NOC-QXN dovrà supportare sono classificate in:

- **Funzionalità di front – office**, comprendenti:
  - **Provisioning Tecnico dei servizi**:
    - servizio di front-office per il recepimento da parte delle richieste di accesso al servizio da parte dei fornitori SPC;
    - assegnazione ai fornitori assegnatari delle risorse richieste (ad esempio, porte sugli switch su cui attestare il BR);
    - realizzazione delle infrastrutture e configurazione della QXN;
    - gestione del piano di indirizzamento e delle politiche di routing, in armonia con la gestione di rete di ciascun fornitore assegnatario;
    - definizione del modeling di rete per la raccolta dei dati necessari all'alimentazione dei successivi processi di supporto (monitoraggio QoS ed assistenza tecnica).
  - **Assistenza Tecnica**:
    - servizio di Call Center per la raccolta delle segnalazioni pervenute;
    - servizio di Help Desk di II livello, rivolto ai referenti dei fornitori assegnatari e del CG-SPC;
    - attività di Trouble Ticketing per la gestione dei disservizi;

- servizio di fault monitoring proattivo;
- coordinamento delle attività di assistenza e manutenzione on-site, in accordo con i NAP ospitanti, sia per le attività straordinarie che per gli interventi che non richiedono interruzione del servizio.

- **Funzionalità di back – office**, comprendenti:
  - **Consulting Tecnico**:
    - supporto al provisioning di nuovi accessi;
    - supporto alle attività di assistenza tecnica;
    - presidio dell'evoluzione tecnologica e di servizio della QXN.
  - **Network & System Management**:
    - monitoraggio dell'HW e del SW installato, nonché delle risorse trasmissive;
    - monitoraggio degli eventi critici e superamento soglie su parametri di controllo predefiniti;
    - ottimizzazione e tuning degli apparati di rete;
    - gestione e monitoraggio dei sistemi di back-up;
    - gestione e monitoraggio dei database di sistema.
  - **Security Management**:
    - controllo e verifica degli eventi di sicurezza;
    - controllo e verifica della protezione fisica delle risorse;
    - controllo e verifica della protezione logica delle informazioni;
    - gestione degli incidenti;
    - sviluppo e manutenzione dei sistemi hardware e software utilizzati nel realizzare le policy di sicurezza del SPC.
- **Funzionalità di supporto**, comprendenti:
  - **Performance Management**: consente la raccolta di dati analitici relativi alle misure di traffico, alla qualità dei servizi erogati ed alla rispondenza ai SLA definiti in ambito QXN.
  - **Configuration Management**: consente la gestione del modeling di rete relativo ai servizi erogati ai fornitori assegnatari (inserimento/attivazione e modifica/variazione).
  - **Fault Monitoring***:* consente di centralizzare le segnalazioni/allarmi di fault provenienti dalla QXN nel suo complesso.
  - **Trouble Ticket Management**: consente la gestione ed il tracciamento delle segnalazioni di disservizio a partire dall'apertura del guasto fino alla sua risoluzione.
  - **Repository dei dati**: prevede la raccolta centralizzata di tutti i dati utili alla predisposizione dei report contrattuali e tecnici (modeling, piani di indirizzamento, misure di performance, etc.). Per motivi di affidabilità tutti i dati dovranno essere duplicati su adeguate strutture di back-up.
  - **Sorgente del tempo ufficiale di rete:** prevede la fornitura in rete attraverso uno o più indirizzi pubblici visibili sul SPC del tempo ufficiale di rete attraverso il protocollo Network Time Protocol NTP versione 3 (cfr. RFC 1305) per consentire la sincronizzazione dei sistemi dei fornitori SPC, del CG-SPC ed eventualmente delle

amministrazioni. Il servizio dovrà essere erogato su Hardware e Software ridondato per garantire un'affidabilità di almeno il 99,99% ed essere sincronizzato periodicamente con con il tempo di riferimento nazionale dell'Istituto Elettrotecnico Nazionale "Galileo Ferraris".

Infrastruttura del NOC-QXN

Il NOC-QXN dovrà essere situato in locali adeguati ad ospitare sistemi informativi e dotati di pavimento flottante. I locali dovranno essere dotati almeno dei seguenti dispositivi:

- di rivelazione fumi e spegnimento incendi;
- anti-allagamento;
- anti-intrusione;
- di condizionamento;
- di continuità ed emergenza;
- di controllo degli accessi fisici.

Su tutti i sistemi dovranno essere predisposte opportune politiche di back-up, ridondanza e recovery periodico dei dati.

Le connessioni fra il NOC-QXN e la QXN dovranno essere realizzate garantendo meccanismi di sicurezza ed affidabilità tali da impedire intrusioni fisiche e logiche da parte di personale non autorizzato.

Il NOC-QXN dovrà interfacciarsi con il CG-SPC secondo le specifiche descritte nel capitolo 5 .

Disaster Recovery

Il NOC-QXN dovrà essere in grado di assicurare l'erogazione dei servizi di gestione anche a fronte di eventi eccezionali che ne impedissero il funzionamento. La SC-QXN dovrà implementare una soluzione tecnica che consenta di garantire il ripristino delle funzionalità basilari di configuration management, fault management e network management secondo i livelli di servizio previsti.

Il NOC-QXN dovrà effettuare periodicamente dei back-up completi dei sistemi in modo tale da mantenere l'allineamento dei dati e consentire il recupero della gestione delle funzionalità in caso di necessità. Il NOC-QXN dovrà collaborare con il CG-SPC per effettuare periodiche simulazioni per la verifica della procedura di Disaster Recovery volte a controllare:

- stato di allineamento dei sistemi informativi;
- capacità di reazione;
- tempi di ripristino della funzionalità di gestione;
- corretta implementazione di tutte le procedure.

La SC-QXN dovrà nominare all'interno del NOC-QXN un **Responsabile Operativo della sicurezza** che dovrà fungere da punto di contatto prioritario per tutte le problematiche di sicurezza che interessano l'infrastruttura della QXN. Il Responsabile Operativo della sicurezza potrà avvalersi di sostituti i cui nominativi dovranno essere preventivamente comunicati al CG-SPC.

6.4 Caratteristiche dei nodi della QXN

6.4.1 Caratteristiche logiche

Dal punto di vista logico, la struttura dei nodi della QXN si divide in tre livelli:

- livello infrastrutturale, su cui poggia la rete di trasporto L3;
- livello di peering, su cui poggia la rete locale L2 per il peering;
- livello di accesso, costituito dagli accessi dei fornitori SPC alla QXN.

La struttura di ogni nodo della QXN, dovrà rispecchiare la logica dei tre livelli ed essere costruita con criteri di ridondanza a garanzia della continuità del servizio. Tutte le apparecchiature che partecipano alla QXN, siano esse in gestione alla QXN o al fornitore assegnatario, dovranno comunque essere ad uso esclusivo del servizio offerto dalla QXN.

6.4.2 Caratteristiche tecniche

La realizzazione dei livelli infrastrutturale, di peering e di accesso, dovrà assicurare le seguenti caratteristiche:

- **Ridondanza**: gli apparati che compongono i singoli livelli, le interconnessioni tra un livello e l'altro nonché le interconnessioni tra i nodi della QXN e quelle tra i fornitori assegnatari e la QXN dovranno essere ridondati affinché siano evitati i single point of failure, ossia un singolo malfunzionamento non sia causa di fermo dell'intera infrastruttura su quel nodo.
- **Accessibilità per il controllo remoto**: trattandosi di un'infrastruttura distribuita, ogni apparato che compone i livelli infrastrutturali e di peering dei nodi della QXN dovrà essere accessibile da remoto per operazioni di manutenzione ordinaria, straordinaria e di controllo.

Caratteristiche tecniche del livello infrastrutturale

Per ogni nodo della QXN, il livello infrastrutturale dovrà essere composto da almeno una coppia di apparati IP/MPLS configurati in modo tale da garantire il bilanciamento di carico ed in grado di gestire l'intero traffico del nodo in caso di guasto di uno degli apparati.

Il nodo dovrà essere interconnesso con almeno i seguenti collegamenti:

- doppia interconnessione verso il livello di peering; ognuna di queste interconnessioni dovrà essere realizzata almeno a velocità di 1 Gb/s su apparati distinti;
- interconnessione multipla verso i nodi remoti: a prescindere dalle modalità e dalle tecnologie da utilizzarsi sulla rete di interconnessione geografica tra i nodi della QXN, ciascuno di questi dovrà essere connesso ad altri nodi della rete con almeno 2 collegamenti.

Dovrà essere possibile al CG-SPC l'accesso in letture alle MIB degli apparati del livello infrastrutturale.

Caratteristiche tecniche del livello di peering

Per ogni nodo il livello di peering dovrà essere composto da almeno due switch con componenti ridondate ed essere in grado di gestire l'intero traffico del nodo in caso di guasto di uno degli apparati e così interconnessi:

- doppia connessione verso il livello di trasporto;
- doppia interconnessione tra gli switch, realizzata su porte appartenenti a moduli distinti;
- le connessioni verso i BR del fornitore del livello di accesso saranno connessioni doppie con velocità fisica a 1 Gb/s.

Gli switch dovranno supportare funzionalità e sistemi di mirroring avanzati, nonché protocolli standard per la partecipazione delle porte a diverse VLAN ed essere conformi agli standard internazionali rispetto alla gestione dei pacchetti a livello 2. In particolare gli switch dovranno implementare tecniche standard per la gestione di qualità di servizio a livello 2 (ad esempio 802.1p).

A livello progettuale potrà essere considerata l'ipotesi di utilizzare una sola coppia di apparati per realizzare contemporaneamente i livelli logici di peering ed infrastrutturale.

Caratteristiche tecniche del livello di accesso

Il livello di accesso, a carico del fornitore assegnatario, dovrà essere inteconnesso con il livello di peering almeno tramite una doppia interfaccia LAN a 1 Gb/s.

Domini di responsabilità

La SC-QXN ed i fornitori assegnatari saranno responsabili della manutenzione di ogni componente del proprio dominio di competenza e saranno abilitati ad operare esclusivamente su tali componenti.

Il **dominio di competenza della SC-QXN** è rappresentato dagli apparati (router, switch, server, etc.) che costituiscono il livello infrastrutturale ed il livello di peering di ogni nodo, delle interconnessioni locali tra tali apparati e di quelle geografiche tra i nodi della QXN e da tutte le infrastrutture che alloggiano le apparecchiature della QXN e dei fornitori assegnatari.

Il dominio di competenza della SC-QXN termina sul collegamento del livello di peering sulla porta del BR del fornitore SPC.

Il **dominio di competenza di ciascun fornitore SPC** è definito dalle apparecchiature (router) del fornitore SPC che collaborano al livello di accesso e termina sulla porta degli apparati del livello di accesso dei fornitori SPC.

Caratteristiche della rete di trasporto QXN

Il dimensionamento della rete di trasporto dovrà essere basato su dati ricavati dal monitoraggio dei volumi di traffico scambiati sulla rete in modo da pianificare tempestivamente gli aggiornamenti dei link di interconnessione tra i nodi della QXN. Dovranno essere garantite le seguenti caratteristiche:

- i collegamenti tra i nodi della QXN dpvranno garantire la completa magliatura della rete;
- il dimensionamento dei link dovrà garantire che l'occupazione media dei link, misurata su ogni intervallo di 5 minuti, non superi il 50% della capacità del collegamento; al superamento della soglia le capacità dei collegamenti dovranno essere ripianificate;
- il dimensionamento dei link dovrà garantire il rispetto delle prestazioni riportate definite come SLA anche in caso di guasto di uno dei nodi o di uno dei collegamenti.

6.4.3 Criteri di scelta dei NAP

La SC-QXN dovrà individuare almeno due NAP presso i quali co-locare i nodi della QXN. I NAP dovranno possedere le seguenti caratteristiche organizzative e tecniche:

- interconnettere fornitori in possesso di regolare autorizzazione ministeriale, dotati di un proprio AS e di un proprio spazio di indirizzi IP;
- operare con caratteristiche di neutralità nei confronti dei fornitori assegnatari e degli operatori trasmissivi e non svolgere alcuna attività in concorrenza con essi;
- operare in base a chiare e pubbliche politiche di adesione e di utilizzo della propria infrastruttura;
- essere raggiunto da almeno 3 diversi operatori di telecomunicazioni che offrono circuiti sul territorio italiano;
- avere in gestione esclusiva le sale che ospitano il NAP pubblico e che rispondono ai requisiti di sicurezza funzionale di cui al paragrafo 6.6 ;
- garantire che i locali, sede del NAP pubblico, siano atti all'installazione di apparecchiature elettroniche e di telecomunicazione e che non vi siano vincoli architettonici o di altra natura che inficino l'erogazione del servizio;
- disporre di spazi adeguati per ospitare gli apparati della QXN;
- garantire un presidio H24, con personale opportunamente selezionato, finalizzato a segnalare anomalie rispetto alle condizioni di esercizio ordinario;
- garantire l'esistenza di adeguata polizza assicurativa circa i rischi di responsabilità civile.

La SC-QXN dovrà contrattualizzare con i NAP prescelti un servizio di housing che preveda le seguenti prestazioni:

- gli armadi, le apparecchiature contenuti nel NAP ed i collegamenti elettrici e telefonici degli stessi dovranno essere indenni da manomissioni e da malfunzionamenti dovuti ad incuria o negligenza da parte di terzi;
- le apparecchiature dovranno essere indenni da interruzioni dell'alimentazione elettrica e della funzionalità delle linee telefoniche e di trasmissione dati collegate agli armadi stessi, che dipendano direttamente dal NAP pubblico;
- la disponibilità di funzionamento della sala e dei servizi tecnologici della QXN contenuti nel NAP (impianti di condizionamento, gruppi di continuità, etc.) non dovrà essere inferiore al 99,9% su base mensile;
- il personale che opera sulle apparecchiature della QXN dovrà avere l'accessibilità alla sede con formula 24x7x365. I criteri di sicurezza dovranno comprendere almeno l'identificazione del personale attraverso un documento di riconoscimento valido (utilizzando ad esempio badge magnetico o smart card).

6.5 Indirizzamento della QXN

Il piano di indirizzamento della QXN dovrà garantire l'univocità degli indirizzi IP attribuiti ai singoli sistemi che, connessi tramite la QXN, scambieranno traffico tra loro.

La QXN dovrà essere dotata di un proprio Autonomous System pubblico (ASQ).

Gli annunci BGP verso AS connessi alla rete della QXN dovranno rispettare le regole definite dal Comitato Tecnico della SC-QXN (cfr. paragrafo 6.3.2).

6.6 La sicurezza della QXN

6.6.1 Sicurezza fisica

Le misure di sicurezza fisica riguardano le aree in cui sono presenti gli apparati dei fornitori oggetto dei servizi di housing erogati dall'infrastruttura QXN (cfr. paragrafo 6.2), gli apparati della QXN e del relativo sistema di gestione.

La SC-QXN dovrà garantire le seguenti misure di sicurezza fisica:

- **Aree ad accesso controllato.** Tutti i locali contenenti apparati della QXN o del relativo sistema di gestione dovranno essere ad accesso controllato (cfr. paragrafo 6.4.3). L'accesso ai locali dovrà avvenire solo a seguito del riconoscimento dell'operatore.

  Le pareti degli edifici dovranno essere in muratura o in materiale di robustezza equivalente e le porte di accesso ai locali dovranno essere di adeguata robustezza. Inoltre le eventuali finestrature dovranno essere protette mediante vetri antisfondamento (e infissi di robustezza adeguata) o grate di protezione.

  Le aree dovranno essere perimetrate con pareti di media robustezza (ad esempio in muratura semplice) di altezza superiore ai 2 metri.

- **Antiscavalcamento.** Le aree ad accesso controllato dovranno essere protette da un sistema di protezione passiva antiscavalcamento sulla recinzione perimetrale di sufficiente robustezza. Il sistema di protezione passivo antiscavalcamento potrà essere sostituito da un allarme attivo antiscavalcamento (ad esempio di tipo a microonde o a doppia tecnologia) o da un allarme attivo per la protezione perimetrale.

- **Sistemi di allarme.** Le aree contenenti apparati della QXN o del relativo sistema dovranno essere protette, con misure anti-intrusione, contro atti dolosi tendenti a trafugare, danneggiare le apparecchiature o interrompere il servizio. Dovrà essere previsto un rilevatore di battente aperto per porte e finestre (ad esempio del tipo a contatto magnetico a triplo bilanciamento antistrappo).

  Le finestrature dovranno essere provviste di sistema di rilevazione effrazione (ad esempio mediante rilevatori di vibrazioni). L'interno del sito dovrà essere protetto da un sistema di rivelazione presenze.

  Dovrà essere presente un sistema di segnalazione degli allarmi di tipo locale o remoto.

  Dovrà essere inoltre presente un sistema di guardiania o di reception durante l'orario di lavoro oppure una postazione remotizzata di supervisione supportata dal sistema di televisione a circuito chiuso (TVCC). Il sistema TVCC potrà essere interno al sito (di tipo fisso) o esterno in prossimità di porte e finestre con un sistema di videoregistrazione in funzione 24 su 24.

  I rivelatori ed i segnalatori di allarme dovranno essere protetti da azioni di sabotaggio (ad esempio mediante custodie antivandalo e sistemi di interrogazione dei rilevatori con crittografia delle informazioni). Le centraline di allarme dovranno essere collocate in postazione remota e protette.

Ogni tentativo di effrazione dovrà essere immediatamente rilevato e segnalato al personale addetto alla sorveglianza.

- **Controllo dell'accesso ai locali.** Dovrà essere previsto un registro elettronico interno delle visite contenente, per ogni visita:
  - nome e cognome del visitatore;
  - persone da visitare;
  - data e ora di ingresso;
  - data e ora di uscita.

  Il registro elettronico dovrà inoltre essere in grado di gestire una black list dei visitatori cui non è consentito l'accesso ai locali. Il personale interno ed ogni visitatore dovranno essere muniti di badge. Il badge dovrà essere consegnato previa presentazione di un documento personale di identità. Il varco di accesso ai locali dovrà essere di tipo mono-utente (ad esempio mediante tornelli a tripode o (a sbarra). i visitatori o gli autoveicoli in ingresso dovranno essere identificati a livello di reception o di guardiania. Nel caso di siti senza reception o guardiania l'autorizzazione all'ingresso dovrà essere data esclusivamente mediante attivazione del badge. Nel caso in cui il visitatore sia diretto presso un'area non presidiata, dovrà essere controllato durante la sua permanenza all'interno dell'area.

  Per l'accesso ai locali contenenti i router della QXN dovrà essere previsto l'utilizzo di un badge a prossimità attivato da un PIN con scadenza annuale.
- **Impianti elettrici**. Gli impianti elettrici, dimensionati secondo le esigenze operative, dovranno seguire le procedure previste dalla L.96/1990 e dovrà essere previsto un piano di manutenzione ordinaria. Dovrà inoltre essere prevista una procedura per l'effettuazione di test del sistema elettrico ad intervalli programmati.

  Dovranno essere previste linee separate sotto continuità elettrica.

  Tutti gli apparati della QXN dovranno essere protetti nei confronti dei problemi relativi all'alimentazione elettrica con sistemi che assicurino un elevato periodo di autonomia (almeno 4 ore).
- **Condizionamento e ventilazione.** I locali destinati ad ospitare gli apparati della QXN dovranno essere dotati di un sistema di climatizzazione automatica, dotato di sensori di temperatura.

  Il sistema di condizionamento provvede al filtraggio dell'aria, alla ventilazione interna, al raffreddamento e riscaldamento mediante aria fresca esterna, garantendo quindi la giusta temperatura ed il sufficiente ricambio d'aria.

  Il sistema di condizionamento dovrà garantire il rispetto dei parametri indicati nella tabella seguente:

Parametri ambientali	Unità di misura	Valori
Velocità di incremento e decremento della temperatura	°C/min	0,5
Pressione minima	K Pa	70
Pressione massima	K Pa	106
Irraggiamento solare	W/m2	700

Irraggiamento termico	W/m2	600
Movimento dell'aria circostante	m/s	5

Tabella 29: Sicurezza fisica della QXN

Le anomalie nella temperatura dei locali dovranno essere segnalate da un sistema di allarme ottico o acustico di tipo locale e remoto.

La manutenzione del sistema di climatizzazione dovrà essere effettuata ad intervalli pianificati, dovranno inoltre essere previsti test periodici di efficienza.

- **Anti incendio**. Le aree destinate ad ospitare gli apparati della QXN dovranno essere protette contro gli incendi mediante idonee misure di rilevazione ed intervento.

  L'impianto dovrà prevedere sensori di rilevazione fumo collocati nell'ambiente.

  I sistemi di allarme dovranno prevedere avvisatori ottici ed acustici. La centralina di allarme dovrà prevedere l'individuazione puntuale dell'area in cui si è sviluppato l'eventuale incendio e l'allarme dovrà essere remotizzato su un sinottico ad indirizzo collettivo. La centralina dovrà essere protetta da eventuali azioni di sabotaggio e da eventuali sovratensioni.

  Il circuito di controllo dovrà essere ridondato per evitare interruzioni nei collegamenti.

  Dovrà essere previsto l'inoltro dell'allarme al più vicino comando dei VVFF.

- **Anti Allagamento**. Le aree destinate ad ospitare gli apparati della QXN dovranno essere protette contro gli allagamenti mediante idonee misure di rilevazione ed intervento. Nel caso i locali si trovino a livello stradale o inferiore, dovranno essere previsti sistemi anti-allagamento dotati di opportune pompe idrauliche. Inoltre, nel caso di siti ad elevato rischio di allagamento (ad esempio in prossimità di fiumi), dovrà essere previsto un sistema di sentine per lo smaltimento, dotato di alimentazione autonoma.
- **Cablaggi.** I cavi dovranno essere protetti da possibili atti vandalici (sistemi antistrappo) e da possibili deterioramenti (posa in canaline o corrugati). Nel caso di locali con rischio di allagamento, la posa cavi dovrà essere aerea o a soffitto.

  Le terminazioni dei cavi elettrici dovranno essere legate, in modo tale da non lasciare cavi sciolti sul pavimento.

  I cavi dei singoli cablaggi dovranno essere facilmente rintracciabili, ispezionabili ed estraibili. Inoltre dovrà essere disponibile uno schema di cablaggio costantemente aggiornato.
- **Protezione degli apparati attivi.** Gli apparati attivi dovranno essere compartimentati mediante armadi di cablaggio con chiusura a chiave; dovrà inoltre essere previsto un sistema di rilevazione battente porta aperto con avvisatore.

  Gli armadi di cablaggio dovranno essere dotati di ventole di areazione e di un sistema interno di rilevazione temperatura. Gli armadi di cablaggio dovranno essere compartimentati per tipologia di apparati in essi contenuti.

6.6.2 Sicurezza logica

La SC-QXN dovrà assicurare le seguenti misure minime di sicurezza logica relative alla protezione degli apparati di rete:

- **Identificazione ed autenticazione degli operatori.** Tutti gli apparati della QXN (router, sistemi di gestione e sistemi di protezione) dovranno essere dotati di una funzione di Identificazione ed Autenticazione in grado di identificare e autenticare univocamente gli operatori che accedono ai fini della gestione (network management).

  Il sistema di sicurezza dovrà essere capace di individuare e amministrare il diritto di accesso degli operatori, o di gruppi di operatori, ai dati e ai servizi nonché le regole e i processi per ogni specifico oggetto. Per ogni tentativo di accesso da parte di operatori ad oggetti sottoposti al controllo accessi, il sistema di sicurezza dovrà verificarne il diritto e la validità.

  Dovrà essere presente un sistema di amministrazione delle utenze in grado di gestire i profili di accesso alle funzioni di ogni utente. Il profilo d'accesso dovrà basarsi sull'identificativo (user-id) dell'utente. Il controllo accessi alle funzioni dovrà basarsi su una politica di controllo accessi "chiusa" (tutto ciò che non è esplicitamente concesso è vietato), inoltre non dovrà essere consentita la propagazione dei diritti di accesso.

- **Tracciamento**:
  - **Tracciamento delle attività di amministrazione della rete**. Gli apparati di rete dovranno essere un grado di registrare le operazioni di amministrazione della rete eseguite dagli operatori (previa autorizzazione preventiva delle rappresentanze sindacali interne, secondo quanto previsto dall' art. 4 dello Statuto dei lavoratori). La granularità delle registrazioni dovrà essere configurabile da utenti autorizzati. Non dovrà essere permesso agli utenti non autorizzati di accedere alle informazioni registrate.
  - **Tracciamento del traffico di rete**. Tutte le apparecchiature di rete dovranno essere dotate di funzioni di log. Dovranno essere disponibili funzioni che permettano di rilevare selettivamente il traffico (in funzione delle caratteristiche dei pacchetti) e strumenti automatici per eseguire indagini e verificare le situazioni anomale. L'attività di registrazione dei log dovrà essere personalizzabile in funzione delle politiche di sicurezza. I log di registrazione del traffico dovranno essere conservati per il periodo di tempo massimo consentito dalla normativa in vigore sulla protezione dei dati personali (Codice in materia di protezione dei dati personali - D.L. 30 giugno 2003 n.196).
- **Gestione upgrade del SW.** Gli avanzamenti di release non dovranno mai essere attuati contemporaneamente su tutti gli apparati della rete o su tutti gli apparati di un singolo nodo, per evitare il rischio che eventuali problemi relativi al nuovo release riguardino l'intera rete.
- **Protezione nei confronti degli attacchi al protocollo BGP.** Dovranno essere adottate misure che riducano i rischi di attacco al protocollo BGP prevedendo almeno l'uso di funzioni di hash MD5 (Message Digest Algorithm v.5) per l'autenticazione dei pacchetti o protezioni equivalenti.
- **Sezionamento dei collegamenti.** Dovrà essere possibile discriminare e, se necessario, isolare, i collegamenti tra i nodi della QXN ed i nodi di reti non ritenute affidabili mediante sistemi di firewalling od opportune liste di controllo.
- **Network IDS**. Presso i punti di accesso ai nodi della QXN dovrà essere installato un prodotto di tipo Network IDS in grado di rivelare possibili tentativi di attacco alla rete.

6.6.3 Norme e procedure per la sicurezza

La SC-QXN dovrà garantire il rispetto delle norme e delle procedure di sicurezza minima di gestione della QXN elencate di seguito:

- **Hardening ed Integrità del software.** Dovranno essere previste specifiche procedure per la configurazione dei sistemi operativi e del software di base e per la verifica della loro integrità nei confronti delle modifiche non autorizzate. In particolare, in fase di prima installazione ed in occasione di successivi adeguamenti, dovrà essere attuata una configurazione che riduca il numero delle funzioni disponibili minimizzando i rischi di uso non corretto degli apparati.

  Dovrà inoltre essere previsto un processo di gestione degli aggiornamenti e di controllo periodico della loro integrità.
- **Rilevamento degli attacchi sistematici.** Dovranno essere attivate opportune procedure che permettano di rilevare quando un apparato è sottoposto ad attacco sistematico. Dovrà inoltre essere prevista una procedura di pronta reazione e di allarme che preveda il tempestivo coinvolgimento del Responsabile Operativo della sicurezza della QXN**.**
- **Test ciclici di impenetrabilità.** La SC-QXN dovrà verificare attraverso test, senza arrecare danno ai dati ed ai servizi, l'efficacia delle misure di sicurezza attuate. In accordo con il CG-SPC la SC-QXN dovrà eseguire test periodici di impenetrabilità su tutte le apparecchiature di rete della QXN. Dovranno essere utilizzati tool, specializzati e allo stato dell'arte, per individuare le debolezze della rete e/o dei sistemi e/o dei servizi. Dopo ogni test dovranno essere messe in atto le opportune azioni correttive. La SC-QXN dovrà comunicare al CG-SPC i risultati dei test e le azioni correttive messe in atto.
- **Disposizioni formali.** Dovranno essere rese disponibili al personale interessato istruzioni scritte inerenti i seguenti aspetti della gestione della sicurezza:
  - accesso fisico delle persone agli edifici in cui sono situati apparati della QXN o del relativo sistema di gestione;
  - accesso fisico delle persone ai locali contenenti apparati della QXN o del relativo sistema di gestione;
  - regole per l'accesso da parte di personale esterno (fornitori, addetti alla manutenzione e visitatori);
  - gestione degli strumenti per l'accesso a casseforti ed armadi blindati (combinazioni delle casseforti, chiavi degli armadi, etc.);
  - gestione degli archivi cartacei (regole per la conservazione, modalità di consultazione, eventuale registrazione degli accessi, etc.);
  - gestione di situazioni anomale;
  - ripristino dell'interruzione dell'erogazione di energia elettrica;
  - procedure di backup e di restore.
- **Auditing interno**. Dovranno essere previste verifiche interne circa il rispetto delle norme e delle procedure delineate.

6.7 Manutenzione della QXN

Per interventi di **manutenzione ordinaria** si intendono tutte le operazioni che possono essere pianificate con anticipo. Per interventi di **manutenzione straordinaria** si intendono tutte le operazioni che non possono essere pianificate con anticipo.

Ogni qualvolta sia necessario effettuare un intervento di manutenzione sul dominio di competenza della SC-QXN, questa dovrà informarne tutte le altre parti coinvolte (fornitori SPC, CG-SPC) specificando data ed ora prevista dell'intervento, durata prevista dello stesso ed indicando una breve descrizione del tipo di intervento e se questi preveda una interruzione del servizio. Tale comunicazione dovrà essere effettuata via posta elettronica e confermata telefonicamente:

- con almeno 5 giorni di anticipo in caso di manutenzione ordinaria;
- con almeno 4 ore in caso di interventi di manutenzione straordinaria.

In ogni caso dovrà anche essere segnalata la chiusura delle operazioni, specificando l'ora in cui l'intervento è stato portato a termine.

6.8 Gestione del periodo transitorio

Durante il periodo precedente la piena operatività della QXN i fornitori assegnatari, per poter erogare i servizi (sia OPA che OPO), dovranno utilizzare, come punto temporaneo di interconnessione, la rete locale del Punto di Interconnessione della RUPA (PIR). Tramite il PIR sarà altresì accessibile un collegamento all'interdominio della RUPA che consentirà di veicolare il traffico da e verso le amministrazioni ancora attestate sulla RUPA durante la fase di attivazione dei servizi SPC.

Durante il periodo di esercizio della QXN e finché non sia completata la migrazione delle amministrazioni dalla RUPA al SPC, la QXN dovrà prevedere un collegamento tra uno dei nodi della QXN ed il PIR. Tale collegamento dovrà essere dimensionato secondo gli stessi criteri di dimensionamento e di affidabilità previsti per i collegamenti interni della QXN, e rimanere in attività almeno fino alla realizzazione completa della QXN stessa e, a richiesta del CNIPA, fino al completamento del periodo in cui il CNIPA stesso provvederà al rimborso dei costi sostenuti dalla SC-QXN, secondo quanto previsto dallo Schema di Contratto CNIPA-Società Consortile QXN (allegato 4).

PARTE SECONDA – COLLAUDI E DOCUMENTAZIONE DI RISCONTRO

7 COLLAUDI

Nel presente capitolo sono descritte tutte le procedure di collaudo che il fornitore assegnatario dovrà attuare ai fini della verifica della completa funzionalità dei servizi erogati.

7.1 Prescrizioni generali

La fornitura dei servizi descritti nel presente capitolato tecnico dovrà essere soggetta alle seguenti procedure di collaudo:

a) Servizi di connettività e sicurezza:

- **Collaudo funzionale su piattaforma tecnica, test bed** (cfr. paragrafo 7.2): è svolto dal CNIPA; il Contratto Quadro prevede delle prove mirate a verificare le modalità con le quali il fornitore erogherà i servizi di connettività (cfr. capitolo 1) e sicurezza (cfr. capitolo 2) oggetto della presente gara..
- **Collaudo di configurazione** (cfr. paragrafo 7.3): è svolto dalla singola amministrazione interessata; ogni contratto esecutivo stipulato tra il fornitore assegnatario e l'amministrazione prevede delle prove mirate a verificare la corretta erogazione dei servizi acquisiti dall'amministrazione attraverso la compilazione del "Piano dei fabbisogni dell'amministrazione" (cfr. paragrafo 4.1).

b) QXN:

- **Collaudo della QXN (**cfr. paragrafo 7.4), svolto dal CNIPA prevede delle prove mirate a verificare la rispondenza tecnica e funzionale di quanto realizzato rispetto al Progetto approvato dal CNIPA e la corretta erogazione dei servizi.

7.2 Collaudo funzionale su piattaforma tecnica (test bed)

In seguito alla stipula del Contratto Quadro con il CNIPA, il fornitore assegnatario dovrà progettare e realizzare una **piattaforma tecnica (test bed)** al fine di consentire al CNIPA l'esecuzione di una prova di collaudo atta a verificare la conformità dei servizi SPC erogati a quanto richiesto dal presente Capitolato Tecnico (cfr. capitoli 1 e 2) e ad eventuali modifiche concordate in corso d'opera nell'ambito del Comitato Operativo e/o del Comitato di Direzione Tecnica.

Il fornitore assegnatario dovrà realizzare la piattaforma di test bed presso sedi individuate congiuntamente con il CNIPA, strutturandola in modo tale da consentire al CNIPA l'esecuzione delle verifiche funzionali per tutti i servizi oggetto del Contratto Quadro. Il fornitore assegnatario dovrà fornire anche il personale necessario all'esecuzione delle prove.

Il fornitore assegnatario dovrà consegnare al CNIPA un documento intitolato ***"Specifiche di dettaglio delle prove di collaudo dei servizi in ambiente di prova (test bed)"*** contenente almeno (cfr. paragrafo 8.2.1):

- descrizione architetturale della piattaforma tecnica (test bed);
- elenco delle prove di collaudo, con particolare riferimento a:

    - servizi di trasporto;
    - servizi VoIP;
    - servizi di supporto;
    - servizi di interoperabilità;
    - architettura, servizi e politica di sicurezza;
- sistema di misura dei livelli di servizio e di generazione della reportistica;
- funzionalità ed architettura del NOC/SOC del fornitore assegnatario;
- modalità di svolgimento delle prove di collaudo.

7.3 Collaudo di configurazione

In seguito alla stipula del Contratto Esecutivo con la singola amministrazione, il fornitore assegnatario dovrà supportare l'amministrazione nell'esecuzione di una prova di collaudo "sul campo" atta a verificare la conformità delle caratteristiche di ogni singolo PAS consegnato all'amministrazione:

- alle indicazioni contenute nel "Piano dei fabbisogni" redatto dalla singola amministrazione (cfr. paragrafo 4.1);
- al progetto del fornitore assegnatario descritto nel "Progetto dei fabbisogni" (cfr. paragrafo 4.2);
- alle specifiche contenute nel presente Capitolato Tecnico;
- ai risultati delle verifiche su test bed (cfr. paragrafo 7.2).

Il fornitore assegnatario dovrà 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 (cfr. paragrafo 8.2.2).

Le prove di collaudo dovranno verificare almeno:

- caratteristiche HW/SW e funzionalità dei sistemi installati;
- interfaccia rete interna (PAS);
- connettività end-to-end e verifica della corretta implementazione delle CdS richieste nella sede;
- servizi di sicurezza implementati;
- rilevazioni sugli indicatori di qualità del servizio;
- procedure di fatturazione e rendicontazione.

Il fornitore assegnatario dovrà altresì impegnarsi, qualora richiesto dall'amministrazione, a svolgere ulteriori prove integrative. L'amministrazione potrà procedere, a sua discrezione, ad un collaudo a campione.

7.4 Collaudo della QXN

Il CNIPA, di concerto con i fornitori assegnatari costituenti la SC-QXN, effettuerà una prova di collaudo atta a verificare la conformità dei servizi erogati dalla rete di interconnessione, secondo quanto specificato nel capitolo 6 .

La prova di collaudo sarà svolta presso la sede e le strutture della SC-QXN o in quelle dei fornitori assegnatari utenti dei servizi della stessa, pertanto i fornitori assegnatari dovranno mettere a disposizione del CNIPA gli ambienti di collaudo.

Il collaudo sarà effettuato secondo le modalità descritte nel documento intitolato ***"Progetto della QXN"*** (cfr. paragrafo 8.1).

In particolare il collaudo della QXN riguarderà la rispondenza tecnica e funzionale di quanto realizzato rispetto al Progetto approvato dal CNIPA ed almeno:

- i servizi di erogati dalla QXN (cfr. paragrafo 6.2);
- i requisiti, funzionalità ed architettura del NOC-QXN (cfr. paragrafo 6.3.3);
- i requisiti dei nodi della QXN (cfr. paragrafo 6.4);
- i piani di indirizzamento della QXN (cfr. paragrafo 6.5);
- le caratteristiche di sicurezza della QXN (cfr. paragrafo 6.6).

8 DOCUMENTAZIONE DI RISCONTRO

Nel presente capitolo sono elencati i documenti che dovranno essere redatti e gestiti rispettivamente da:

- SC-QXN (cfr. paragrafo 8.1);
- fornitore assegnatario (cfr. paragrafo 8.2).

Il fornitore assegnatario dovrà inviare tutta la documentazione di seguito descritta in formato elettronico (almheno in formato .pdf). E' facoltà dei destinatari della documentazione richiedere l'invio della stessa anche in formato cartaceo.

Tutta la documentazione tecnica relativa ai servizi di seguito descritta dovrà essere conforme alla norma UNI EN ISO 9004-2 ed in particolare dovrà 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.

8.1 Documentazione a carico della SC-QXN

La SC-QXN dovrà predisporre, aggiornare in corso d'opera (e, comunque, ad ogni cambiamento dei sistemi utilizzati), gestire e rendere disponibile la documentazione di riscontro delle attività svolte, nei contenuti previsti dal contratto esecutivo stipulato fra il CNIPA e la SC-QXN (cfr. allegato 4).

Documento di riscontro	Contenuto	Riferimento Capitolato Tecnico
Progetto della QXN	• Piano temporale di realizzazione della QXN (identificazione delle attività necessarie all'attivazione dei servizi, pianificazione temporale dettagliata, risorse allocate, stato di avanzamento lavori, identificazione dei rischi e piano di recovery).	Capitolo 6

	• Piano della sicurezza. • Specifiche di controllo di prestazioni, dei livelli di servizio e della qualità. • Schema di convenzione di adesione ai servizi.	
Progetto di dettaglio della QXN	• Specifiche di dettaglio della sicurezza (architetture, sistemi utilizzati, policy implementate). • Specifiche tecniche della QXN (architettura, sistemi utilizzati, dimensionamento dei collegamenti, piano di indirizzamento, modalità tecniche di colorazione del traffico, regole di instradamento del traffico). • Specifiche di collaudo dei servizi erogati dalla QXN (elenco delle prove di collaudo, tempi dei collaudi, composizione della Commissione, eventuali problemi insorti in fase di collaudo e soluzioni adottate). • Livelli di servizio e penali.	Allegato 4
Documento di organizzazione della SC-QXN	• Descrizione della struttura funzionale ed organizzativa della SC-QXN • Nomi dei responsabili per ognuna delle aree funzionali • Procedure di escalation per ogni funzione interessata.	paragrafo 6.3
Preventivo e consuntivo per la realizzazione della QXN	• Elenco dei prodotti/sistemi/servizi per la realizzazione e la gestione della QXN con i relativi costi	Allegato 4

Tabella 30: Documentazione di riscontro a cura della SC-QXN

La SC-QXN dovrà inoltre predisporre un documento intitolato **"Manuale della Qualità"** in accordo con le seguenti linee guida:

- conservare i principi generali di qualità adottati dai fornitori assegnatari ("Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi", cfr. paragrafo 8.2.2);
- fare proprie quelle parti del documento "Specifiche di dettaglio della realizzazione dei servizi richiesti e specifiche di controllo della qualità degli stessi" che siano applicabili al

contratto di cui è fornitrice, adattando, se fosse necessario, le procedure al contesto di utilizzo;

- integrare il documento elaborato dai fornitori assegnatari con quanto non compreso ma richiesto dal contesto.

Le implementazioni al Manuale della Qualità dovranno tenere conto di quanto previsto dalla normativa ISO sulla assicurazione e gestione della qualità, in particolare nel settore della Information Technology.

Il Manuale della Qualità costituirà il riferimento per l'assicurazione e la gestione della qualità nel contratto da parte della SC-QXN e costituirà documento di riscontro per il monitoraggio sui processi.

8.2 Documentazione a carico del fornitore assegnatario

Il fornitore assegnatario dovrà predisporre, aggiornare in corso d'opera (e, comunque, ad ogni cambiamento dei sistemi utilizzati), gestire e rendere disponibile la documentazione di riscontro delle attività svolte, nei contenuti previsti dal contratto quadro (cfr. allegati 2 e 3).

8.2.1 Documentazione relativa al Contratto Quadro OPA/OPO

L'elenco della documentazione di riscontro che dovrà essere predisposta dal fornitore assegnatario è riportato nella tabella seguente con l'indicazione, per ciascun documento, dei contenuti di particolare interesse:

Documento di riscontro	Contenuto	Riferimento Capitolato Tecnico	Destinatario
Documento programmatico di gestione della sicurezza	• Descrizione delle misure organizzative (ruoli, responsabilità e procedure), tecniche (sistemi hw e sw impiegati) e fisiche adottate per soddisfare i requisiti del paragrafo 1.5.2 .	paragrafo 1.5.2	CNIPA e CG-SPC
Piano generale per l'erogazione dei servizi	• Descrizione della struttura funzionale ed organizzativa del fornitore assegnatario 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.	-	CNIPA

Documentazione tecnica relativa all'erogazione dei servizi di trasporto	• Caratteristiche delle TdR: - Dimensioni di ingombro degli apparati e spazi complessivi necessari, comprese le aree di disimpegno per una 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 (always-on, dial-up, wireless). • Descrizione dell'infrastuttura di rete utilizzata per l'erogazione dei servizi.	paragrafo 1.1	CNIPA, CG-SPC e amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa al servizio DNS	• Numero, tipologia e caratteristiche tecniche dell'hardware utilizzato per erogare il servizio. • Tipologia e release del software utilizzato per erogare il servizio.	paragrafo 1.2.2	CNIPA, CG-SPC e amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa al servizio VoIP	• 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.	paragrafo 1.3	CNIPA, CG-SPC e amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa al 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.	paragrafo 1.4.1	CNIPA, CG-SPC e amministrazioni che acquisiscono il servizio

	• Caratteristiche dei collegamenti tra la rete del fornitore assegnatario ed i sistemi utilizzati per erogare il servizio.		
Documentazione tecnica relativa ai servizi di Data Center	• Marca, tipo e modello dell'apparato definito per la fornitura del servizio. • Sistema operativo e sistemi software necessari all'erogazione del servizio (es: Web Server). • Eventuale sistema di clustering implementato per soddisfare i livelli di servizio indicati negli allegati 2c e 3a. • Modalità di alimentazione delle pagine Web per il servizio di hosting. • Sistema di gestione utilizzato.	paragrafo 1.4.3	CNIPA, CG-SPC e amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa al servizio di Manutenzione e Assistenza dei servizi di connettività	• Descrizione architetturale e funzionale deò NOC. • 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 assegnatario ed i sistemi utilizzati per erogare il servizio.	paragrafo 1.5	CNIPA, CG-SPC 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 assegnatario ed i sistemi utilizzati per erogare il servizio. • Meccanismi/protocolli utilizzati per realizzare l'integrazione con altri strumenti di sicurezza forniti dal fornitore assegnatario o da terzi, la modalità e il livello di integrazione.	paragrafo 2.2	CNIPA, CG-SPC e amministrazioni che acquisiscono il servizio
Documentazione tecnica relativa al servizio di Manutenzione e Assistenza dei servizi di sicurezza	• Descrizione architetturale e funzionale deò SOC. • Numero, tipologia e caratteristiche tecniche dell'hardware utilizzato per erogare il servizio. • Tipologia e release del software utilizzato	paragrafo 2.12	CNIPA, CG-SPC e amministrazioni che acquisiscono il servizio

	per erogare il servizio.		
Documentazione tecnica relativa al servizio di formazione	• Curriculum Vitae dei docenti. • Piano dei corsi. • Certificazioni dei docenti.	paragrafo 1.5.8 e 2.12.8	CNIPA e amministrazioni
Specifiche di dettaglio delle prove di collaudo dei servizi in ambiente di prova (test bed)	• Architettura del test-bed. • Elenco delle prove di collaudo.	paragrafo 7.1	CNIPA

Tabella 31: Documentazione di riscontro relativa al Contratto Quadro OPA/OPO

8.2.2 Documentazione relativa al Contratto Esecutivo OPA/OPO

Documento di riscontro	Contenuto	Riferimento Capitolato Tecnico	Destinatario
Progetto dei fabbisogni	• Descrizione della nuova rete della amministrazione. • Piani di indirizzamento delle amministrazioni. • Regole di traduzione di indirizzi (NAT) in rapporto con la QXN. • Dimensionamento dei servizi/accessi. • Modalità di attivazione dei servizi di connettività/sicurezza.	paragrafo 4.2	Amministrazioni
Costi (parte integrante del Documento "Progetto dei fabbisogni")	• Dettaglio dei costi del progetto previsto dal Piano di Attuazione secondo quanto riportato nell'allegato 2d.	paragrafo 4.2	Amministrazioni
Modalità di presentazione e approvazione degli Stati di Avanzamento Mensili (parte integrante del Documento "Progetto dei fabbisogni")	• Punti di accesso installati. • Esito dei collaudi effettuati e collaudi previsti nel mese successivo. • Varianti e modifiche emerse nel periodo. • Ritardi verificatisi nelle attivazioni rispetto alle date previste nel Piano di Attuazione del Progetto dei Fabbisogni. • Malfunzionamenti verificatisi nel periodo.	paragrafo 4.2	Amministrazioni

	• Tempi di risposta del Call Center. • Tempi di intervento e ripristino dei malfunzionamenti. • Disponibilità complessiva ed unitaria del servizio. • Report statistici sul traffico. • Report statistici sulla sicurezza.		
Piano di Attuazione (parte integrante del Documento "Progetto dei fabbisogni")	• Descrizione della struttura funzionale ed organizzativa del fornitore assegnatario 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, etc.) 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.	paragrafo 4.2	Amministrazioni
Piano Operativo (parte integrante del Documento "Piano di Attuazione")	• Pianificazione temporale dettagliata (diagramma di Gantt delle singole attivazioni, schedulazione delle milestones principali, piano dei soprallouoghi, etc.).	paragrafo 4.2	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 assegnatario in fase di erogazione dei servizi richiesti dall'amministrazione.	paragrafo 4.2	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,	paragrafo 4.2	Amministrazioni

	caratteristiche tecniche/dimensionali degli apparati utilizzati, requisiti elettrici, fisici ed ambientali che devono essere previsti nelle sedi dell'amministrazione che ospiterà 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 assegnatario 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 assegnatario 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, etc.) utilizzati dal sistema di assicurazione e controllo qualità.		
Specifiche di dettaglio delle prove di collaudo	• Tipologia di collaudo. • Elenco delle prove di collaudo. • Tempi dei collaudi.	paragrafo 7.3	Amministrazioni

Tabella 32: Documentazione di riscontro relativa al Contratto Esecutivo OPA/OPO