

CLASSIFICAZIONE DEL DOCUMENTO: CONSIP PUBLIC

ALLEGATO 5 CAPITOLATO TECNICO

PREMESSA	4
1 SERVIZIO DI INTERCONNESSIONE QXN (IQXN)	8
1.1 Caratteristiche dei nodi della QXN	12
1.2 Domini di Responsabilità	14
1.3 Indirizzamento	15
1.4 Sicurezza	16
1.5 Profilo di Servizio “Interconnessione QXN OPA”	17
1.6 QoS in ambito OPA	21
1.7 Profilo di Servizio “Interconnessione QXN OPO”	22
1.8 QoS in ambito OPO	26
1.9 Servizio DNS.....	26
1.10 Servizio NTP	30
1.11 Circuiti di Collegamento Geografico	31
1.12 Manutenzione	33
1.13 Sistemi di gestione e misura dei livelli di servizio	33
2 SERVIZI PER L’INTEROPERABILITÀ DELLE APPLICAZIONI (SIA)	35
2.1 Servizio di Certificazione (SPKI)	36
2.2 Servizio di Gestione del Repertorio Nazionale dei Dati Territoriali (RNDT)	37
2.3 Servizio Indice della Pubblica Amministrazione (IPA)	51
2.4 Servizio Indice dei Gestori PEC (IGPEC)	59
3 SERVIZI DI GOVERNANCE (SGOV)	62
3.1 Servizio di Gestione Automatizzata dei Contratti (SGAC)	69
3.2 Servizio di Gestione dei Dati di Qualità e Sicurezza (SGQS)	74
3.3 Servizio di Gestione delle Escalation (SGES)	76
3.4 Servizio di Gestione dell’Accesso Web (SGAW)	77
4 SERVIZI DI SUPPORTO ALL’OPERATIVITÀ (SSOP)	89
4.1 Organizzazione	93
4.2 Sicurezza	94
4.3 Strutture di supporto	96
4.4 Strumenti di supporto	101
4.5 Servizi di sviluppo	104

5	MODALITÀ DI ATTIVAZIONE DEI SERVIZI	108
5.1	Progetto Esecutivo	108
5.2	Collaudo	110
5.3	Documentazione di riscontro	111
6	MISURAZIONE DEI LIVELLI DI SERVIZIO E REPORTISTICA	113

Premessa

- [D.1] Il presente documento formula i requisiti minimi per la progettazione, realizzazione, fornitura e gestione operativa dei servizi delle Infrastrutture Nazionali Condivise del Sistema Pubblico di Connettività e Cooperazione (SPC² o anche, nel seguito del documento, SPC2) e le modalità con le quali tali servizi dovranno essere erogati.
- [D.2] La numerazione delle specifiche segue il formato [X.N] dove:
- X indica la classe del requisito, secondo la seguente classificazione:
 - Punti di natura definitoria e/o interpretativa, indicati con il carattere “D”, con lo scopo di agevolare la corretta interpretazione delle specifiche illustrate nel documento stesso;
 - Prescrizioni che dovranno essere soddisfatte nell’offerta, indicate con il carattere “R”, con specifico impegno da parte del concorrente.
 - N è un numero progressivo.
- [D.3] Nel seguito si indicherà con il termine "Fornitore" l’aggiudicatario della presente gara.
- [R.1] I servizi e le forniture oggetto di gara riguardano:
- 1) Servizio di interconnessione QXN (IQXN), le cui specifiche sono riportate nel Capitolo 1, in continuità con i servizi erogati alle PA dalla precedente infrastruttura QXN.
 - 2) Servizi per l’interoperabilità delle applicazioni, le cui specifiche sono riportate nel Capitolo 2:
 - Servizio di certificazione (SPKI);
 - Servizio di gestione del Repertorio Nazionale dei Dati Territoriali (RNDT);
 - Servizio Indice della Pubblica Amministrazione (IPA);
 - Servizio Indice dei gestori PEC (IGPEC).
 - 3) Servizi di Governance, le cui specifiche sono riportate nel Capitolo 3:
 - Servizio di gestione automatizzata dei contratti (SGAC);
 - Servizio di gestione dei dati di qualità e sicurezza (SGQS);
 - Servizio di gestione delle escalation (SGES);
 - Servizio di gestione dell’accesso web (SGAW).
 - 4) Servizi di supporto all’operatività, le cui specifiche sono riportate nel Capitolo 4.



- [R.2] Per tutte le forniture in favore di AgID previste nel presente documento, è fatto obbligo al Fornitore, per l'intera durata contrattuale, di prestare il servizio di manutenzione correttiva e, comunque, eseguire tutte le attività e prestazioni che si rendessero necessarie per garantire i livelli di servizio previsti nell'appendice "SLA e penali".
- [R.3] Nei casi in cui il presente documento non specifichi in modo univoco le modalità di erogazione di un particolare servizio o di un suo elemento, il concorrente dovrà evidenziare nell'offerta le modalità che intende adottare per la fornitura del servizio o del suo elemento.
- [R.4] I servizi di cui al requisito [R.1] punti 2 e 3 devono essere co-locati in un **unico data center** di cui al requisito di capacità tecnica riportato al punto 17.3 lett. b) del bando di Gara, e quindi con certificazione in corso di validità del Sistema di Gestione per la Sicurezza delle Informazioni relativamente alle attività di gestione e/o conduzione di centri elaborazione dati, rilasciata in conformità alla ISO/IEC 27001 da un ente di certificazione accreditato da ACCREDIA o da altro ente di Accreditamento firmatario degli accordi di Mutuo riconoscimento per lo schema "Sistemi di gestione per la sicurezza delle informazioni – ISMS". Qualora previsto dal piano di Disaster Recovery di cui al [R.284] e [R.350], i servizi di cui al requisito [R.1] punti 2 e 3 possono prevedere l'utilizzo di un **data center secondario**, solo se anche tale secondo data center possiede la certificazione di cui sopra.
- [R.5] **Collegamento Infranet:** è fatto obbligo al Fornitore di realizzare l'interconnessione tra i nodi della QXN di Roma e Milano (cfr. [R.20]) ed i data center di cui al requisito [R.4] con livello di affidabilità elevato e dimensionata in modo tale da soddisfare, nel complesso, gli SLA previsti per ciascun servizio erogato dai suddetti data center.
- [R.6] **Collegamento Internet:** l'interconnessione tra i data center di cui al requisito [R.4] ed Internet deve essere realizzata per il tramite di due differenti Internet Service Provider. L'interconnessione inoltre deve essere dimensionata in modo tale da soddisfare, nel complesso, gli SLA previsti per ciascun servizio erogato dai suddetti data center.
- [R.7] **Sicurezza:** le infrastrutture condivise (il data center di cui al requisito [R.4] e i nodi QXN) devono prevedere dei sistemi di sicurezza perimetrale, in alta affidabilità, sia a protezione dei collegamenti di cui al requisito [R.5] sia a protezione dei collegamenti di cui al requisito [R.6] e funzionali alla sicurezza dei servizi ospitati. In particolare devono essere implementate in entrambi i casi almeno le seguenti caratteristiche minime:
- Servizio di controllo del flusso tramite firewall
 - Servizio di Network Intrusion Detection/Prevention
 - Servizio di monitoraggio e registrazione degli eventi di sicurezza

[R.8] Il Fornitore deve riservare un Autonomous System (AS) pubblico, eventualmente coincidente con quello definito in [R.40], ed uno spazio di indirizzamento IP pubblico dedicato ai servizi di cui al requisito [R.4]. Tali risorse devono essere assegnate ad AgID e gestite dal Fornitore. Il Fornitore deve elaborare un piano di indirizzamento dei servizi di cui al requisito [R.4] che deve garantire il raggiungimento dei singoli servizi al medesimo indirizzo IP dai diversi ambiti SPC. Di seguito una schematizzazione della topologia dei suddetti servizi:

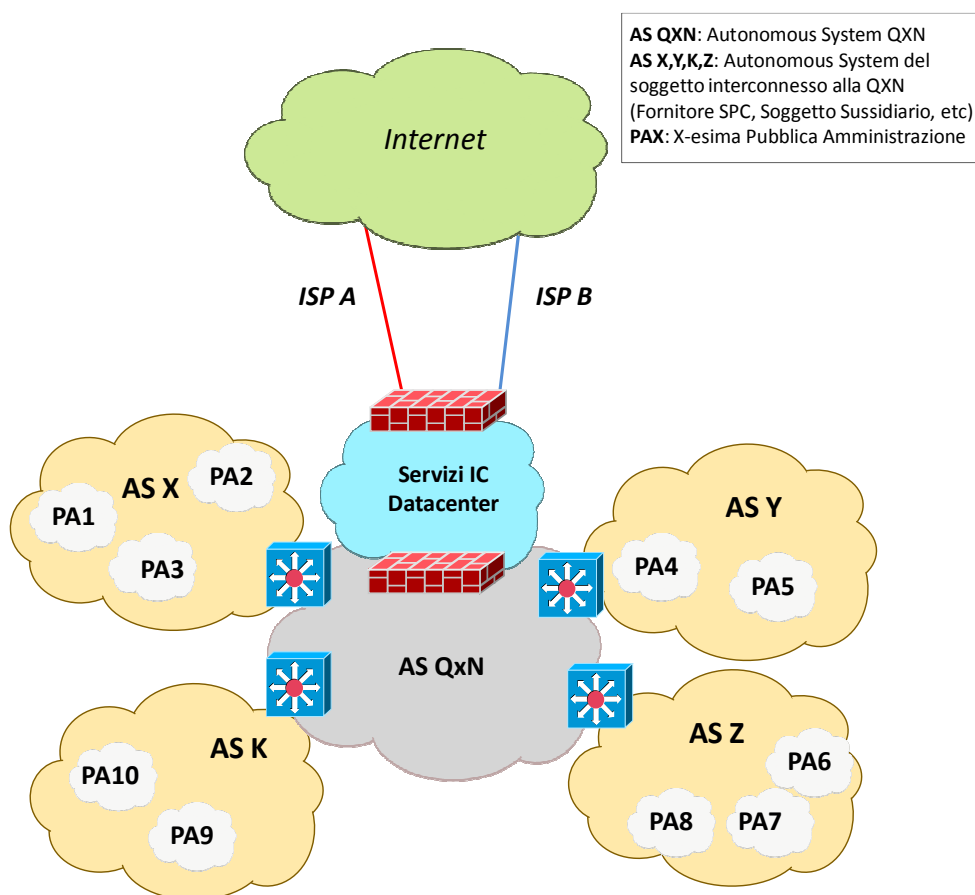


Figura 1

[R.9] Tutta la documentazione progettuale, organizzativa e tecnica prodotta durante l'esecuzione delle attività contrattuali, ivi compresa quella redatta e presentata dal Fornitore durante il procedimento di gara, saranno di proprietà di AgID senza limitazioni di alcun tipo. AgID potrà utilizzare e riutilizzare completamente ed in parte quanto prodotto, anche durante il periodo di vigenza del contratto e prima della sua scadenza. Qualora lo ritenga opportuno, AgID potrà, senza alcuna limitazione, memorizzare, riprodurre, condividere e distribuire tali documenti a terzi. Tutto il software realizzato dal

fornitore nell'ambito dell'erogazione dei servizi di cui al presente capitolato, ivi compreso il codice sorgente e relativa documentazione, sarà di proprietà di AgID.

- [R.10] Tutti i servizi descritti nel presente capitolato devono essere erogabili tramite indirizzamento e Record DNS sia IPv4 che IPv6.
- [R.11] Alla scadenza o risoluzione del presente Contratto il Fornitore si impegna a porre in essere tutte le attività necessarie o utili al fine di permettere la migrazione dei servizi offerti al nuovo Fornitore subentrante. In ogni caso, il Fornitore dovrà assicurare la continuità della prestazione dei servizi attuando eventuali modifiche operative, indicate da AgID, al fine di pianificare il passaggio graduale dei servizi al nuovo Fornitore subentrante, ivi inclusa l'interconnessione con quest'ultimo (a cura e spese di quest'ultimo) per il tempo necessario a completare la migrazione dei servizi sulla sua rete.

1 Servizio di Interconnessione QXN (IQXN)

- [D.4] Le specifiche della precedente infrastruttura QXN e dei relativi servizi di Interconnessione QXN, assimilabili alle forniture ed ai servizi oggetto della presente gara, sono descritti nella documentazione di riscontro QXN-SCPA, in appendice 2 al presente Capitolato e di seguito elencata:
- 1) Specifica del Servizio InterConnessione di QXN (QXN-InterC-SpecificaServizio.pdf);
 - 2) Specifica del Servizio DNS della QXN (QXN-DNS-SpecificaServizio.pdf);
 - 3) Specifica di Realizzazione del servizio InterConnessione QXN (QXN-InterC-SpecRealizzazione.pdf);
 - 4) Specifica di Realizzazione del Servizio DNS della QXN (QXN-DNS-SpecificaRealizzazione.pdf);
 - 5) Specifica di Controllo InterConnessione QXN (QXN-InterC-Specifica Controllo.pdf).
- [R.12] Il Fornitore dovrà progettare, realizzare e fornire ad AgID, nonché gestire, l'infrastruttura **Qualified eXchange Network (QXN)**, volta all'interoperabilità dei Servizi di Connettività SPC². Un estratto della documentazione della procedura ristretta per l'affidamento di tali Servizi di Connettività, è contenuto nell'appendice 7. Attraverso l'infrastruttura QXN il Fornitore dovrà erogare il **Servizio di Interconnessione QXN (IQXN)**, costituito dai Profili di Servizio di cui al requisito [R.16]. Le caratteristiche tecniche dell'infrastruttura da realizzare e fornire ad AgID sono specificate nel presente capitolato.
- [R.13] Il Fornitore deve garantire l'erogazione del Servizio IQXN, secondo quanto stabilito dai requisiti [R.17] e [R.18], ai seguenti soggetti:
- a) **Fornitori della gara per i Servizi di Connettività SPC²**: soggetti individuati per il tramite della gara a procedura ristretta per l'affidamento dei servizi di connettività nell'ambito del Sistema Pubblico di Connettività (CIG 5133642F61 - ID SIGEF 1367) ed obbligati alla sottoscrizione di due Servizi IQXN (uno per ciascuno dei nodi di cui al requisito [R.20]);
 - b) **Altri Fornitori**, di cui all'art 82 del decreto legislativo 7 marzo 2005, n. 82 recante il "Codice dell'amministrazione digitale" e s.m.i., ovvero fornitori Qualificati SPC ai sensi dei regolamenti previsti dall'art. 87 del predetto dLgs;
 - c) **Le Community Network di cui al DPCM 1 aprile 2008**: secondo le modalità di cui all'art. 17 comma 5 lettera a) dello stesso DPCM;
 - d) **Fornitore dei "servizi di telecomunicazione ed informatici per la realizzazione dei servizi e della rete internazionale della pubblica amministrazione" (S-RIPA)**, attuale aggiudicatario del Contratto Quadro n. 5/2010 e, nel prossimo futuro, il fornitore subentrante.

La fruizione del Servizio IQXN da parte di ciascuno dei predetti soggetti avverrà a seguito di sottoscrizione di apposito Contratto Attuativo (rif. Allegato 4B al Disciplinare di Gara) tra il soggetto interconnesso e il Fornitore.

- [R.14] Il servizio IQXN deve permettere l'interconnessione tra i soggetti di cui al [R.13] garantendo il passaggio corretto dei pacchetti IP fra tutti i soggetti connessi a SPC² e deve essere progettato ed erogato in maniera tale da consentire una migrazione graduale e progressiva delle PA dall'attuale al nuovo fornitore di servizi SPC, assicurando la continuità del servizio erogato.
- [R.15] Al fine di consentire la migrazione di cui al requisito [R.14], l'interconnessione tra l'infrastruttura QXN esistente e quella realizzata dal Fornitore è a cura e spese di quest'ultimo.
- [R.16] Il Fornitore ha l'obbligo dell'erogazione, gestione e monitoraggio dei seguenti servizi:
- **Profilo di Servizio "Interconnessione QXN OPA"**: funzionalità di interconnessione ad un singolo nodo QXN per il trasporto del traffico in modalità IP routing (liv. 3 della pila ISO/OSI), ivi compresa la possibilità di disporre, in accordo a quanto stabilito dai requisiti [R.31] e [R.32], di porte FastEthernet, GigabitEthernet e porte 10 GigabitEthernet per l'interconnessione degli apparati di accesso dei soggetti sottoscrittori del profilo di servizio;
 - **Profilo di Servizio "Interconnessione QXN OPO"**: funzionalità di interconnessione ad un singolo nodo QXN per il trasporto del traffico in modalità switching con tecnologia Ethernet (liv.2 della pila ISO/OSI), ivi compresa la possibilità di disporre, in accordo a quanto stabilito dai requisiti [R.31] e [R.32], di porte GigabitEthernet e porte 10 GigabitEthernet per l'interconnessione degli apparati di accesso dei soggetti sottoscrittori del profilo di servizio.
- [R.17] Il Fornitore, a seguito della contrattualizzazione di un profilo di Servizio "Interconnessione QXN OPA" da parte di ciascun soggetto di cui al requisito [R.13], deve garantire, su ogni singolo nodo QXN, i seguenti servizi di supporto dovuti senza oneri aggiuntivi:
- **Servizio Domain Name System (DNS)**: funzionalità di gestione dei nomi di dominio dei soggetti afferenti all'SPC²;

- **Servizio Network Time Protocol (NTP):** funzionalità di sorgente del tempo ufficiale di rete SPC² (tramite protocollo NTP) mediante server sincronizzati al segnale temporale generato dall'Istituto Nazionale di Ricerca Metrologica (I.N.R.I.M.);
- **Servizio di Housing** per l'alloggiamento degli apparati utilizzati dai soggetti sottoscrittori del suddetto profilo di servizio, comprensivo di rack, alimentazione, condizionamento, cablaggio, vigilanza, logistica e pulizia. Lo spazio reso disponibile per il Servizio di Housing deve almeno essere pari a 1/2 rack standard 19" 42 RU, con alimentazione 220V AC su linee ridondate, e comunque non superiore ad 1 rack.

[R.18] Il Fornitore, a seguito della contrattualizzazione di un profilo di Servizio "Interconnessione QXN OPO" da parte dei soggetti di cui al punto a) del requisito [R.13], deve garantire, su ogni singolo nodo QXN, il **Servizio di Housing** (servizio di supporto dovuto senza oneri aggiuntivi) per l'alloggiamento degli apparati utilizzati dai suddetti soggetti, comprensivo di rack, alimentazione, condizionamento, cablaggio, vigilanza, logistica e pulizia. Lo spazio reso disponibile per il Servizio di Housing deve almeno essere pari a 1/2 rack standard 19" 42 RU, con alimentazione 220V AC su linee ridondate, e comunque non superiore ad 1 rack.

[R.19] Il Fornitore deve ospitare il rack e gli apparati dell'operatore che eroga il servizio di interconnessione alla rete STESTA (Secure Trans European Services for Telematics between Administrations) all'interno del data center di cui al requisito [R.4]. Il Fornitore deve inoltre:

- a) Garantire l'interconnessione tra i dispositivi contenuti all'interno del suddetto rack e l'infrastruttura QXN per il tramite del collegamento Infranet di cui al requisito [R.5];
- b) Garantire il supporto necessario all'interconnessione tra il suddetto rack e la rete dell'operatore che eroga il servizio di interconnessione alla rete STESTA (accesso ai locali, cablaggio, etc.);
- c) Effettuare sull'infrastruttura QXN, durante tutta la vigenza contrattuale, le eventuali modifiche al routing, alle regole di network address translation ed alla configurazione dei DNS di QXN secondo le indicazioni che saranno fornite da AgID e volte a garantire la corretta interconnessione tra la rete STESTA e l'ambito Infranet di SPC²;
- d) Nell'ambito del Service Desk di cui al § 4.3, erogare, nei confronti del gestore della rete STESTA, un servizio di incident, availability e security management ed un servizio di gestione delle richieste di accesso ai locali in cui sono ospitati il rack e gli apparati STESTA;

- e) Nell'ambito del NOC e del SOC di cui al § 4.3, eseguire le attività di monitoraggio dell'interconnessione alla rete STESTA, nelle modalità indicate da AgID (sonda ICMP e/o http), e di gestione degli allarmi e dei malfunzionamenti.

[R.20] L'infrastruttura di rete QXN deve avere caratteristiche e compiti simili a quelli di un Internet eXchange Point per il solo traffico scambiato tra le reti dei soggetti di cui al requisito [R.13] e tra tali reti ed i servizi di cui al requisito [R.4]. Deve contemplare una struttura che preveda:

- Architettura geograficamente distribuita con due nodi tra loro interconnessi attraverso collegamenti ridondati di capacità almeno pari a 100 Mb/s;
- I suddetti due nodi dell'infrastruttura QXN (di seguito nodi QXN) devono essere ospitati, per il tramite di contratti stipulati direttamente dal fornitore con i relativi gestori, presso i datacenter dei NAP: MIX s.r.l. di Milano e Consorzio NaMeX di Roma;
- Dimensionamento ed affidabilità dell'infrastruttura adeguati a garantire il rispetto delle caratteristiche di qualità previste da SPC² e definite nell'Appendice "SLA e Penali";
- Funzionalità analoghe a quelle erogate dalla precedente infrastruttura QXN (cfr. [D.4]).

[R.21] Il Fornitore, in merito all'infrastruttura QXN, deve garantire lo svolgimento delle seguenti attività:

- a) Progettazione logica, funzionale ed operativa;
- b) Fornitura di beni e servizi necessari alla realizzazione e all'esercizio;
- c) Definizione delle modalità di collaudo;
- d) Gestione operativa della QXN garantendo nel tempo e per tutta la durata contrattuale l'interconnessione dei soggetti abilitati di cui al requisito [R.13];
- e) Erogazione dei servizi ai soggetti coinvolti;
- f) Progettazione evolutiva, a fronte di nuove esigenze e/o di evoluzione tecnologica.

[R.22] Il Fornitore deve produrre un documento esecutivo denominato "**Regole di Interconnessione QXN**" in cui vengano dettagliatamente descritte le regole tecniche e procedurali cui i soggetti individuati dal requisito [R.13] ed il Fornitore devono attenersi per l'interconnessione alla rete ed ai servizi QXN, ivi compresa la gestione delle attività di provisioning e assurance. Le regole tecniche contenute in tale documento devono garantire la piena interoperabilità tra i soggetti che si interconnettono per il tramite della QXN.

- [R.23] Tutti i dispositivi di rete costituenti l'infrastruttura di rete QXN che saranno collocati presso i due NAP di cui al requisito [R.20], inclusi i dispositivi di sicurezza perimetrale ed i dispositivi per l'erogazione del servizio DNS ed NTP, devono essere ad uso esclusivo del Servizio IQXN.
- [R.24] Il Fornitore deve:
- a) Garantire che per tutti i dispositivi hardware previsti per l'erogazione dei servizi non sia stata annunciata, all'atto della consegna del Progetto Esecutivo, dal vendor tecnologico di riferimento una data di "End of Sale" e/o "End of Support";
 - b) Garantire la costante supervisione del ciclo di vita dei dispositivi hardware e delle release Software utilizzati nell'erogazione del Servizio IQXN, provvedendo ad effettuare tutti gli aggiornamenti necessari all'erogazione del supporto tecnico ed al mantenimento del livello di affidabilità della soluzione adottata;
 - c) Produrre e trasmettere ad AgID un report con la descrizione dell'aggiornamento effettuato a seguito dell'attività di cui al comma precedente.
- [R.25] In qualsiasi momento dell'esecuzione contrattuale la configurazione degli apparati QXN (Router, Switch, Firewall e DNS), su richiesta di AgID, dovrà essere trasmessa ad AgID stessa in apposito formato da concordare tra le parti e su idoneo supporto informatico. Qualora lo ritenga opportuno, AgID potrà utilizzare tali configurazioni senza alcuna limitazione.

1.1 Caratteristiche dei nodi della QXN

- [R.26] Dal punto di vista logico, la struttura dei nodi della QXN deve essere suddivisa in due livelli:
- a) **Livello di routing**, su cui poggia la rete di trasporto L3 (tale livello non è coinvolto nell'erogazione del Profilo di Servizio "Interconnessione QXN OPO" se non per le funzionalità di gestione e monitoring);
 - b) **Livello di switching**, su cui poggia la rete locale L2 per l'interconnessione con i soggetti di cui al requisito [R.13], con i collegamenti geografici di cui al §1.11, con i dispositivi di sicurezza perimetrale di cui al §1.4, con i dispositivi per l'erogazione del Servizio Domain Name System di cui al §1.9 e con il data center di cui al requisito [R.4].
- [R.27] **Caratteristiche tecniche del livello di routing:** Ogni apparato coinvolto nel livello di routing deve:
- a) Supportare i protocolli di routing richiamati all'interno del presente capitolato;

- b) Essere configurato in modo tale da garantire il bilanciamento del carico ed in grado di gestire l'intero traffico IP del nodo in caso di guasto di uno degli apparati;
- c) Supportare standard per la gestione di qualità di servizio a livello IP;
- d) Supportare il protocollo SNMP v3.

[R.28] **Caratteristiche tecniche del livello di switching:** Ogni apparato coinvolto nel livello di switching deve:

- a) Essere in grado di gestire l'intero traffico del nodo in caso di guasto di uno degli apparati;
- b) Supportare funzionalità e sistemi di mirroring avanzati;
- c) Gestire reti LAN virtuali (VLAN) e, qualora necessario, supportare la funzionalità di routing del traffico IP tra VLAN differenti;
- d) Supportare standard per la gestione di qualità di servizio a livello Ethernet (almeno il protocollo 802.1p);
- e) In conformità con quanto definito nel requisito [R.30], essere interconnesso con doppia connessione ai circuiti di collegamento geografico di cui al §1.11;
- f) In conformità con quanto definito nel requisito [R.30], avere una doppia interconnessione a livello di switching con il dispositivo analogo presente nello stesso nodo; tale doppia interconnessione deve essere realizzata su porte appartenenti a moduli distinti del singolo dispositivo, avere una velocità almeno pari a 2 Gb/s e, qualora necessario, consentire upgrade.

[R.29] A livello progettuale deve essere adottata una soluzione basata sull'impiego di un sistema modulare che consenta la coesistenza, in un singolo apparato, dei livelli logici di routing e switching. Tale apparato è convenzionalmente denominato Border Router QXN (BRqxn).

[R.30] La struttura di ogni nodo della QXN deve rispecchiare la logica a due livelli di cui al requisito [R.26] ed essere costruita con criteri di ridondanza ed alta affidabilità a garanzia della continuità del servizio. In particolare deve assicurare le seguenti caratteristiche:

- **Ridondanza fisica e logica:** in ciascuno dei due nodi dell'infrastruttura QXN gli apparati di cui al requisito [R.31], le interconnessioni logiche e fisiche tra gli stessi e verso i soggetti ad essi interconnessi devono essere ridondati affinché siano evitati *single point of failure*.
- **Accessibilità per il controllo remoto:** ogni apparato di cui al requisito [R.31] deve essere accessibile da remoto per le necessarie operazioni di manutenzione.

[R.31] Gli apparati di rete BRqxn devono essere equivalenti o superiori a quelli descritti all'interno del paragrafo "2.1 Apparati di dorsale - BRqxn" del documento "Specifica di Realizzazione del servizio InterConnessione QXN" di cui al [D.4] e devono supportare le seguenti caratteristiche minime:

- a) Capacità massima di forwarding pari a 400 Mpps per il traffico IPv4 e 200 Mpps per il traffico IPv6;
- b) Disponibilità di 48 porte Gigabit Ethernet ottiche (di cui almeno 36 destinate alla connessione dei soggetti di cui al requisito [R.13]);
- c) Disponibilità di 48 porte 10/100/1000 Ethernet rame (di cui almeno 36 destinate alla connessione dei soggetti di cui al requisito [R.13]);
- d) Disponibilità di almeno 4 slot di espansione.

[R.32] Per tutta la durata contrattuale il Fornitore deve effettuare l'upgrade del numero di porte disponibili utilizzando uno degli slot di espansione ed effettuando, previa richiesta di AgID e corresponsione dei corrispettivi previsti, una delle seguenti tipologie di upgrade (su singolo slot di espansione):

- a) Aggiunta di 48 porte 10/100/1000 Ethernet rame;
- b) Aggiunta di 24 porte Gigabit Ethernet ottiche;
- c) Aggiunta di 2 porte 10 Gigabit Ethernet ottiche.

[D.5] Gli apparati di rete dei soggetti che si interconnettono alla rete QXN (cfr. [R.13]) devono supportare tutte quelle funzionalità previste all'interno del documento "Regole di Interconnessione QXN" di cui al requisito [R.22]. Tali apparati sono convenzionalmente denominati Border Router OPA (BRopa), qualora coinvolti nel Profilo di Servizio "Interconnessione QXN OPA", Border Router OPO (BRopo) qualora coinvolti nel Profilo di Servizio "Interconnessione QXN OPO".

1.2 Domini di Responsabilità

[R.33] Il Fornitore ed i soggetti interconnessi ai nodi della rete QXN sono rispettivamente responsabili della manutenzione di ogni componente del proprio dominio di competenza e sono abilitati ad operare esclusivamente su tali componenti.

[R.34] Il dominio di competenza del Fornitore è rappresentato dagli apparati dedicati all'erogazione del Servizio IQXN (router, switch, server, firewall, etc.), dalle interconnessioni locali tra tali apparati, dalle interconnessioni geografiche tra i due nodi della QXN, da tutte le infrastrutture coinvolte nel servizio di housing

(cfr. [R.17] e [R.18]) in cui alloggiano sia le apparecchiature della QXN che quelle dei soggetti interconnessi alla rete QXN.

- [R.35] Il confine del dominio di competenza del Fornitore è individuato nel cassetto ottico e/o dal patch panel UTP installato e mantenuto dal Fornitore stesso all'interno di ciascun rack coinvolto nel servizio di housing (cfr. [R.17] e [R.18]).
- [R.36] La realizzazione e la manutenzione dei cablaggi (ottici e/o elettrici) tra le porte degli apparati BR dei soggetti interconnessi alla rete QXN ed il cassetto ottico o il patch panel di cui al requisito [R.35] sono di competenza dei soggetti medesimi.
- [R.37] La realizzazione e la manutenzione dei cablaggi (elettrici e/o ottici) tra il cassetto ottico o il patch panel UTP di cui al requisito [R.35] e gli apparati BRqxn sono di competenza del Fornitore.
- [R.38] Il dominio di competenza di ciascun soggetto interconnesso a QXN è definito dai propri apparati ospitati in housing (cfr. [R.17] e [R.18]), dalle interconnessioni locali tra tali apparati, dai collegamenti geografici verso la propria rete IP e termina sulla porta del cassetto ottico e/o dal patch panel UTP di cui al requisito [R.35].
- [R.39] Il Fornitore deve provvedere in autonomia a richiedere ed ottenere tutti i permessi necessari all'esecuzione delle opere connesse alla realizzazione dei servizi oggetto della presente procedura, ivi comprese le autorizzazioni per la realizzazione dei cablaggi all'interno dei siti del Mix e del Namex.

1.3 Indirizzamento

- [R.40] L'infrastruttura QXN deve essere dotata di un Autonomous System (AS) pubblico e di uno spazio di indirizzamento IP pubblico dedicato non instradato su internet (sia per IPv4 che per IPv6, cfr. [R.8]). Tali risorse devono essere assegnate ad AgID e gestite dal Fornitore.
- [R.41] Il piano di indirizzamento della QXN deve essere basato su indirizzi IP di cui al requisito [R.40] e deve garantire l'univocità degli indirizzi IP attribuiti ai singoli sistemi costituenti la infrastruttura QXN o ad essa direttamente interconnessi.
- [R.42] Il Fornitore, a richiesta, deve supportare AgID in tutte quelle attività amministrative necessarie per l'assegnazione ad AgID degli indirizzi IP utilizzati nella precedente infrastruttura QXN.

1.4 Sicurezza

- [R.43] Il Fornitore deve progettare, realizzare, fornire e gestire un'infrastruttura di sicurezza composta da apparati gestiti per il tramite del SOC di cui al §4.3. Tale infrastruttura deve assicurare le seguenti funzionalità:
- a) Firewall, 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 basati su funzionalità di tipo "stateful inspection". Il servizio deve supportare tutti i protocolli specificati nello standard TCP/IP e le seguenti caratteristiche di base:
 - Filtraggio di traffico IP, per la protezione da accessi indesiderati bloccando indirizzi, porte o protocolli;
 - Auditing e logging, per consentire l'analisi del traffico che attraversa il firewall;
 - Modulo di gestione che consente di configurare e monitorare il comportamento del sistema firewall;
 - Meccanismi antispoofing;
 - Meccanismi di rilevazione e protezione per attacchi di tipo Denial of Service;
 - Network Address Translation (NAT) secondo la specifica RFC 3022, sia di tipo statico (uno a uno), sia di tipo dinamico (n a uno) e Port Address Translation (PAT);
 - Alta affidabilità in modalità active/standby;
 - b) VPN IPsec Site to Site, per l'interconnessione di reti di management e monitoring;
 - c) Network IDS/IPS, presso i punti di accesso ai nodi della QXN dovrà essere installato un sistema di tipo Network IDS/IPS in grado di rivelare e, laddove possibile, interrompere possibili tentativi di attacco alla rete. Il sistema deve prevedere meccanismi di notifica a fronte dell'identificazione di un evento di attacco;
 - d) I meccanismi di notifica dovranno prevedere, sempre a fronte dell'identificazione di un evento di attacco o comunque di una segnalazione di compromissione, l'inoltro della notifica anche ad un sistema di tipo "syslog server", ad un indirizzo IP comunicato dal CERT-PA;
 - e) Le notifiche di cui al punto d) dovranno viaggiare su canali sicuri, utilizzando gli strumenti definiti al precedente punto b), ovvero utilizzando canali di comunicazione basati su protocolli IPSEC o SSH.
- [R.44] Gli apparati per la protezione dell'infrastruttura QXN con funzionalità di firewall e network IDS/IPS di cui al requisito [R.43] devono essere equivalenti o superiori a quelli descritti all'interno del paragrafo "2.5 Firewall/Network Intrusion Detection System" del documento "Specifica di Realizzazione del servizio InterConnessione QXN" di cui al requisito [D.4].

1.5 Profilo di Servizio “Interconnessione QXN OPA”

[R.45] Il Profilo di Servizio “Interconnessione QXN OPA” consente l’interconnessione a livello 3, per il tramite della rete QXN, dei soggetti attestati alla rete QXN di cui al [R.13] secondo l’architettura schematizzata nella figura seguente:

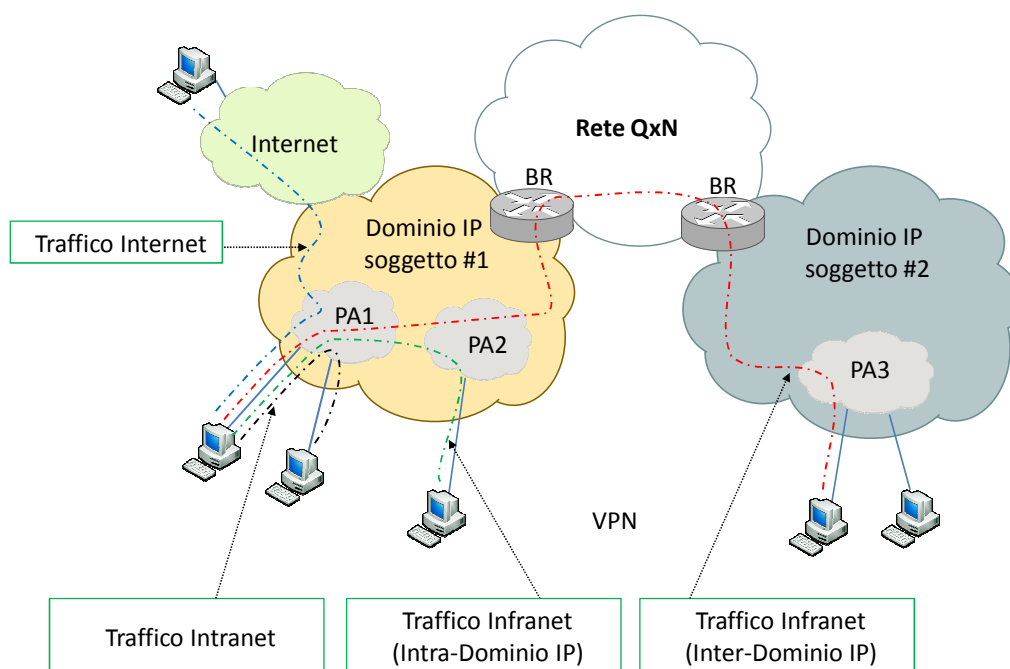


Figura 2

- [R.46] Per il Profilo di Servizio “Interconnessione QXN OPA” è ammesso solo il traffico Intranet. Tale traffico coinvolge due distinti soggetti interconnessi a QXN ovvero i soggetti interconnessi a QXN ed il data center di cui al requisito [R.4].
- [R.47] La rete QXN non deve permettere l’attraversamento del traffico da e per soggetti non attestati al SPC².
- [R.48] Il traffico OPA deve essere gestito e instradato a livello IP. Ai fini dell’interconnessione per il trasporto del traffico Intranet OPA, i BRqxn, ovvero gli elementi di interconnessione che si interfacciano alla rete QXN, agiscono a livello di routing (Livello 3 del modello ISO/OSI).
- [R.49] I BRopa, ovvero gli elementi di interconnessione dei soggetti che si interfacciano alla rete QXN, devono essere co-locati in housing, per il tramite del servizio offerto dal Fornitore (cfr.[R.17]). L’installazione, la gestione e la manutenzione di tali apparati è a carico dei rispettivi soggetti interconnessi.



- [R.50] Il Fornitore deve mantenere aggiornata la configurazione dei BRqxn al fine di ricevere gli annunci delle reti di ciascun soggetto interconnesso alla rete QXN abilitate a scambiare traffico IP per il tramite della QXN.
- [R.51] Il Fornitore deve comunicare ai soggetti interconnessi tutti gli spazi di indirizzamento IP gestiti ed i relativi AS Number, aggiornando contestualmente l'Area informativa QXN di cui al requisito [R.236].
- [R.52] Le Pubbliche Amministrazioni che scambiano traffico all'interno dell'ambito Infranet (ed Internet) SPC² utilizzano uno spazio di indirizzamento IPv4 e/o IPv6 appartenente all'AS del soggetto interconnesso alla rete QXN.
- [R.53] Ciascun soggetto interconnesso alla rete QXN annuncerà ai BRqxn il proprio AS number e lo spazio di indirizzamento (riservato all'interno del suo AS) abilitato a scambiare traffico IP per il tramite della QXN. All'interno dell'infrastruttura QXN il suddetto traffico deve essere bilanciato sui BRqxn che attraversa.
- [R.54] Salvo esplicita comunicazione da parte di AgID, gli annunci dei soggetti interconnessi alla rete QXN non devono avere netmask superiore a 24 bit (non devono essere annunciate subnet contenenti meno di 256 indirizzi IP) e devono garantire il massimo grado di aggregazione.
- [R.55] La rete QXN deve utilizzare l'OSPF come protocollo di routing IGP sia in ambito IPv4 che IPv6. Non deve essere previsto l'uso di aree OSPF diverse dall'area di Backbone ("Area 0" rappresentata in Figura 3).
- [R.56] La rete QXN deve utilizzare il BGP come protocollo di routing EGP (e-BGP) sia in ambito IPv4 che IPv6. Gli apparati della rete QXN devono essere configurati in modalità *fully-meshed* con sessioni i-BGP.

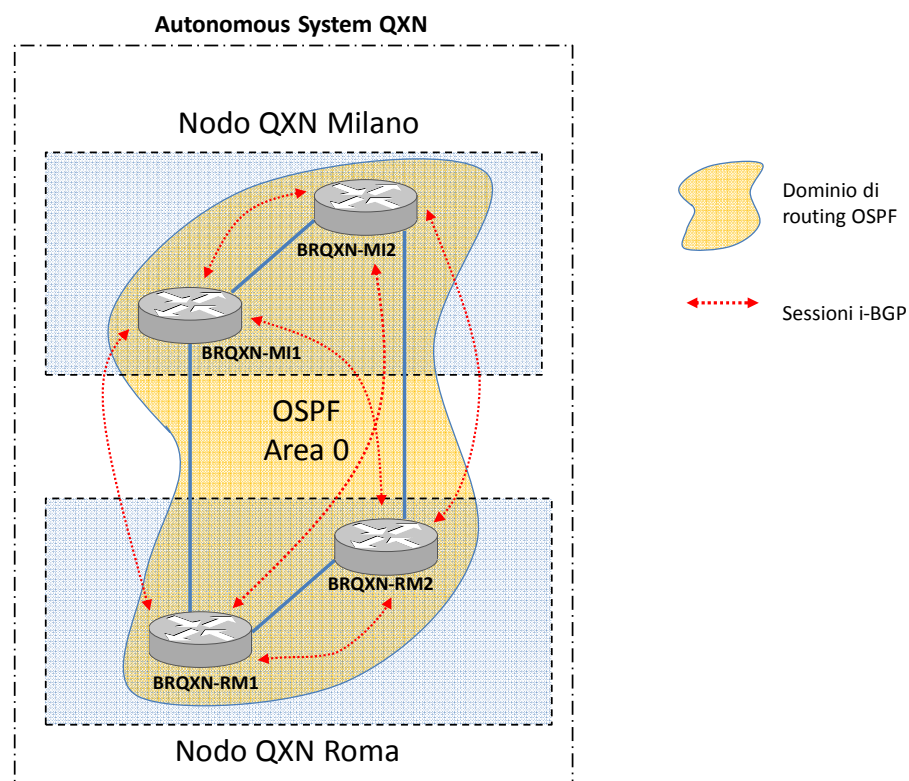


Figura 3

- [R.57] Gli apparati della rete QXN devono avere una sessione e-BGP v.4 con i BR dei soggetti interconnessi alla QXN. L'AS number della rete QXN risulterà l'Autonomous System di transito per il traffico tra i diversi soggetti interconnessi alla rete QXN. Nella seguente figura è riportato lo schema di collegamento di soggetti interconnessi generici ai due nodi dell'architettura QXN di Milano e Roma:

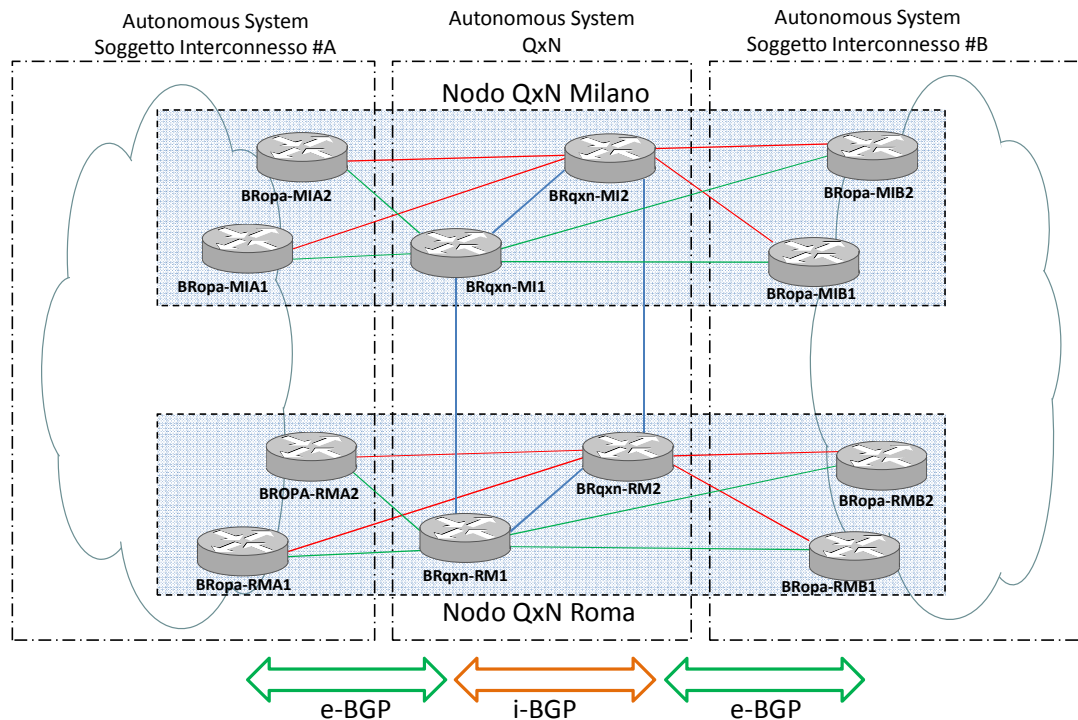


Figura 4

- [R.58] Per garantire la sicurezza ed autenticità degli annunci scambiati tra la rete QxN e quella dei soggetti interconnessi deve essere previsto l'impiego della funzione di hash MD-5 per l'autenticazione dei pacchetti, attivata sui protocolli di routing BGP v.4 e OSPF.
- [R.59] I protocolli di routing OSPF e BGP devono essere configurati in maniera tale da ottimizzare l'affidabilità dell'architettura di rete, garantendo il funzionamento dell'architettura anche a seguito di eventi che determinino l'indisponibilità di uno o più link di interconnessione tra BRopa e BRqxn, fino a contemplare la completa indisponibilità di un nodo QxN.
- [R.60] La soluzione tecnica di interconnessione QxN OPA deve essere recepita all'interno del documento "Regole di Interconnessione QxN" di cui al [R.22], ivi compreso il dettaglio delle attività in capo ai soggetti interconnessi alla rete QxN (cfr. [R.13]) propedeutiche alla corretta realizzazione e gestione della soluzione stessa. In particolare Il Fornitore deve progettare, implementare e recepire all'interno del suddetto documento una soluzione di routing che bilanci simmetricamente il traffico sia in entrata che in uscita alla rete QxN, in analogia a quanto descritto all'interno del paragrafo "2.10.3 Soluzioni di routing per la simmetria del traffico Infranet nativo OPA" del documento "Specifica di Realizzazione del servizio InterConnessione QxN" di cui al [D.4].

1.6 QoS in ambito OPA

- [R.61] Il Fornitore, in ambito OPA, deve implementare meccanismi di gestione della QoS a livello 3 in accordo con la RFC2475 (architettura DiffServ) e con le sue successive integrazioni. Di seguito una rappresentazione dello scenario di riferimento per un singolo collegamento OPA:

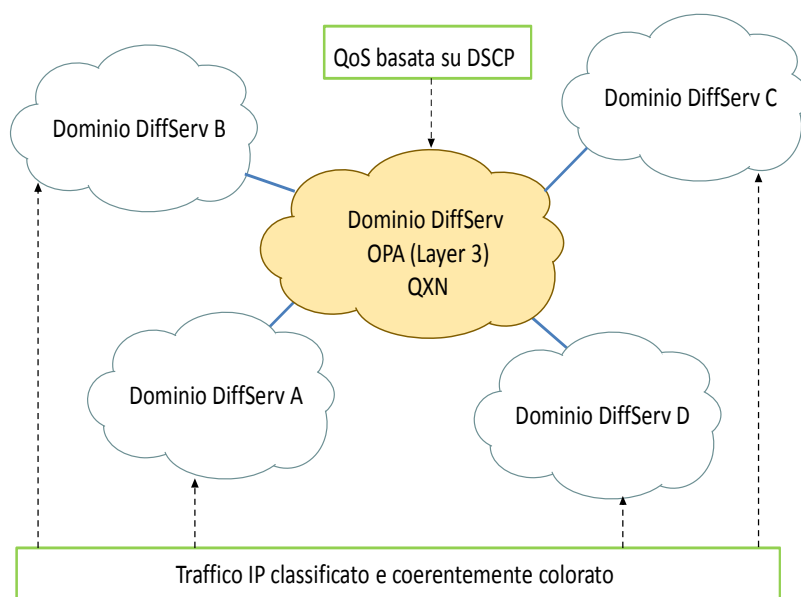


Figura 5

- [R.62] Il Fornitore deve definire e recepire all'interno delle "Regole di Interconnessione QXN" di cui al requisito [R.22] tutte le attività in capo ai soggetti interconnessi alla rete QXN propedeutiche alla corretta gestione della QoS dei collegamenti OPA all'interno del dominio QXN. In particolare il soggetto interconnesso alla rete QXN è responsabile della classificazione e colorazione (attribuzione del valore DSCP) del traffico IP in accordo con la seguente tabella di corrispondenza (per completezza si riporta anche il campo IP Precedence definito dalla RFC 791):

Classe di Servizio	Marcatura mediante IP Precedence (RFC 791)	Marcatura mediante DSCP (RFC 2474)
Real Time	4	CS 4 AF 4x (x=1,2,3)
Mission Critical	3	CS 3 AF 3x (x=1,2,3)
Streaming	2	CS 2 AF 2x (x=1,2,3)

Multimedia	1	CS 1 AF 1x (x=1,2,3)
Best Effort	0	0

Tabella 1

[R.63] In caso di ricezione di valori diversi da quelli indicati nella tabella di cui al [R.62], la QXN deve marcare i pacchetti ricevuti come Best Effort.

[R.64] In considerazione del fatto che, all'interno dell'architettura di rete SPC² sono previste le suddette CoS che devono soddisfare i parametri di qualità *Round Trip Delay* (RTD - tempo di percorrenza necessario ad un pacchetto per percorrere la tratta origine-destinazione-origine), *Packet Loss* (PL - tasso di perdita dei pacchetti, rapporto espresso in percentuale tra il numero di pacchetti non consegnati e numero di pacchetti trasmessi in una tratta origine-destinazione-origine) e *Packet Delay Variation* (PDV - variazione in valore assoluto del ritardo tra due pacchetti consecutivi) in accordo ai valori riportati nella tabella seguente, il Fornitore deve individuare gli opportuni algoritmi da implementare per rendere la rete QXN funzionale e coerente, dal punto di vista di QoS, con l'architettura SPC².

Classe di Servizio	RTD	PL	PDV
Real Time	< 65 ms	< 0,1%	< 10 ms
Mission Critical	< 100 ms	< 0,1%	---
Streaming	< 400 ms	< 0,5%	< 250 ms
Multimedia	< 500 ms	< 5%	---
Multicast *	---	< 0,5%	---

* Solo traffico OPO

Tabella 2

1.7 Profilo di Servizio "Interconnessione QXN OPO"

[R.65] Il Profilo di Servizio "Interconnessione QXN OPO" consente l'interconnessione a livello 2 (protocollo Ethernet), per il tramite della rete QXN, tra il Fornitore Aggiudicatario SPC² ed ogni Fornitore Assegnatario SPC² che abbia sottoscritto un contratto esecutivo OPO della gara multiFornitore SPC². Di seguito una figura che descrive il flusso del traffico OPA scambiato, all'interno della stessa PA in ambito Intranet, per il tramite del servizio OPO.

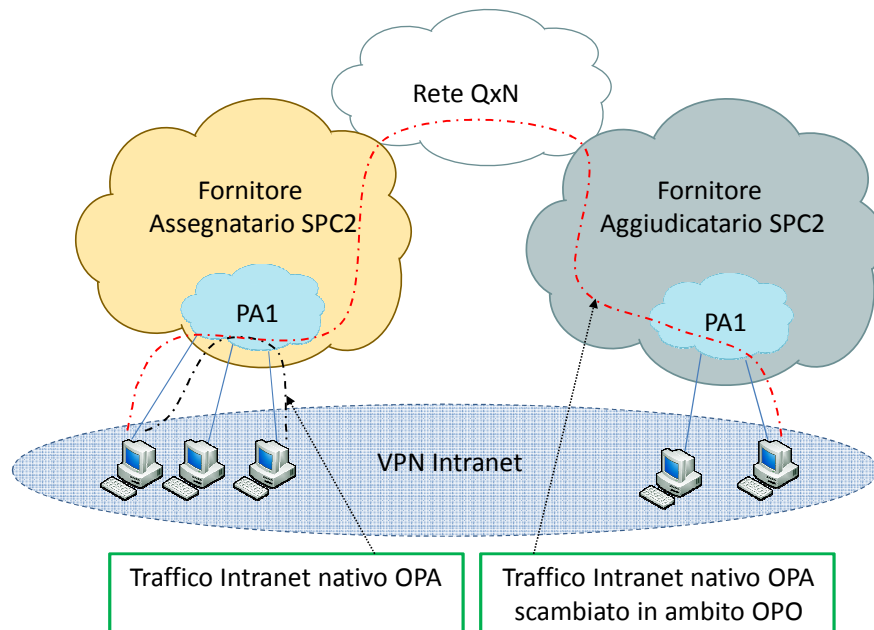


Figura 6

- [R.66] La modalità base di interconnessione prevede che il Fornitore Aggiudicatario SPC² e ciascuno dei fornitori assegnatari SPC² sottoscrittori di un contratto esecutivo OPO interfaccino la propria rete alla rete QxN su entrambi i nodi di Roma e Milano. I BRopo, ovvero gli elementi di interconnessione alla rete QxN, devono essere co-locati in housing, per il tramite del servizio offerto dal Fornitore (cfr. [R.18]). L'installazione, la gestione e la manutenzione di tali apparati è a carico dei rispettivi soggetti interconnessi.
- [R.67] Le porte degli apparati QxN e quelle dei fornitori SPC² dedicate al servizio OPO devono essere configurate in trunk (protocollo IEEE 802.1q).
- [R.68] Su ciascun nodo QxN l'interconnessione OPO deve essere realizzata da ciascun Fornitore SPC² mediante almeno due collegamenti Gigabit Ethernet attestati alla coppia di BRqxn in coerenza con quanto riportato nei requisiti [R.69] e [R.70]. Tali collegamenti devono inoltre soddisfare quanto definito nel requisito [R.71].
- [R.69] La figura seguente schematizza la logica di interconnessione del servizio OPO nel caso in cui il Fornitore Assegnatario decida di schierare una coppia di apparati per il Servizio di Interconnessione QxN OPO su entrambi i nodi QxN (In figura viene utilizzata una nomenclatura puramente indicativa).

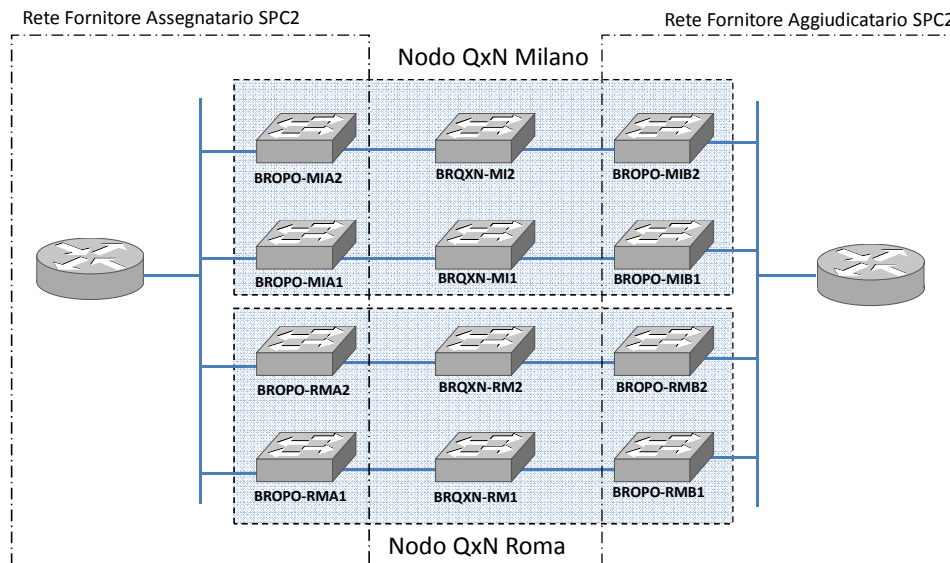


Figura 7

[R.70] La figura seguente schematizza invece la logica di interconnessione del servizio OPO nel caso in cui il Fornitore Assegnatario decida di schierare un solo apparato per il Servizio di Interconnessione QXN OPO su entrambi i nodi QXN. (In figura viene utilizzata una nomenclatura indicativa).

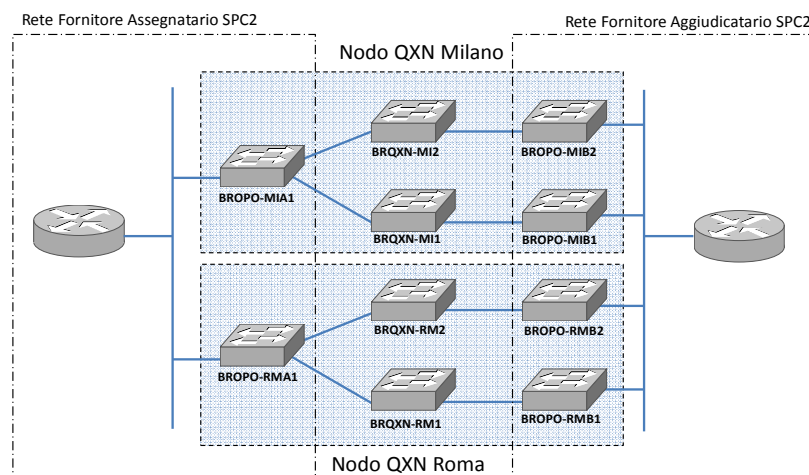


Figura 8

[R.71] Il Fornitore deve progettare una soluzione basata su collegamenti aggregati tra BRqxn e BRopo che consenta di effettuare upgrade di banda e, al contempo, creare una topologia logica priva di loop di livello 2.

[R.72] Il Fornitore deve farsi carico di configurare, all'interno dei dispositivi BRqxn, le VLAN sui differenti trunk OPO in maniera coerente con la procedura di attivazione del servizio OPO di cui al requisito [R.73] (vedasi la figura seguente a titolo esemplificativo).

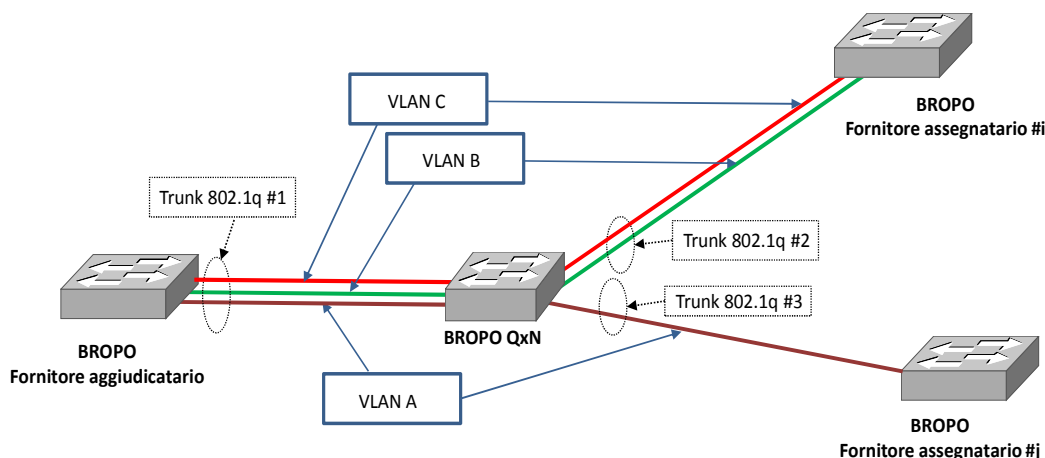


Figura 9

[R.73] **Procedura di Attivazione del Servizio OPO.** La procedura di attivazione del servizio OPO deve rispettare la seguente sequenza logica:

- Configurazione del collegamento OPO tra gli apparati BRqxn del Fornitore e gli apparati BROPO del Fornitore Aggiudicatario SPC²;
- Configurazione, a seguito della sottoscrizione di un contratto esecutivo OPO tra Fornitore Aggiudicatario SPC² e Fornitore Assegnatario SPC², del collegamento OPO tra gli apparati BRqxn del Fornitore e gli apparati del Fornitore Assegnatario SPC² sottoscrittore.
- Configurazione, a seguito della richiesta di attivazione di un nuovo collegamento OPO, degli apparati BRQXN e relativa comunicazione ai soggetti coinvolti (aggiudicatario e assegnatario) delle necessarie informazioni di configurazione.

[R.74] Il Fornitore deve progettare una soluzione in grado di gestire almeno 6.000 collegamenti OPO. Qualora il numero di collegamenti OPO attestati sulla rete del Fornitore Aggiudicatario SPC² ecceda il suddetto valore AgID definirà, dopo aver eseguito un'analisi di fattibilità tecnico-economica condotta congiuntamente ai Fornitori SPC² ed al Fornitore, le modalità di estensione del servizio.

[R.75] La soluzione tecnica di interconnessione QXN OPO deve essere recepita all'interno del documento "Regole di Interconnessione QXN" di cui al [R.22], ivi compreso il dettaglio delle attività in capo ai Fornitori SPC² propedeutiche alla corretta realizzazione e gestione della soluzione stessa.

1.8 QoS in ambito OPO

- [R.76] Il Fornitore, in ambito OPO, deve progettare e implementare una soluzione tecnica che consenta la gestione della QoS a livello 2 e che:
- a) Garantisca gli stessi livelli di disponibilità e qualità del servizio previsti per l'interconnessione OPA;
 - b) Gestisca il traffico di tipo Multicast, previsto nell'ambito Intranet dell'architettura SPC², eventualmente trattandolo alla stregua della classe di servizio Streaming (cfr. [R.64]).
- [R.77] La soluzione tecnica di cui al requisito [R.76] deve essere recepita all'interno del documento "Regole di Interconnessione QXN" di cui al [R.22], ivi compreso il dettaglio delle attività in capo ai Fornitori SPC² propedeutiche alla corretta gestione della QoS dei collegamenti OPO.

1.9 Servizio DNS

- [R.78] In continuità con quanto erogato dalla precedente infrastruttura QXN, il Fornitore deve rendere disponibile un servizio di DNS QXN che consenta la gestione centralizzata dei nomi a dominio relativi allo spazio dei nomi della rete SPC², inteso come l'insieme di tutti i domini pubblicati dalle PA e dai soggetti afferenti al SPC² (c.d. Zone SPC). Il Fornitore dovrà a tal fine progettare, realizzare, fornire e gestire un'infrastruttura che risponda ai requisiti di cui nel seguito.
- [R.79] Il servizio DNS della QXN deve essere reso disponibile a tutti soggetti afferenti alla rete QXN (cfr. [R.13]) attraverso i collegamenti realizzati in ambito Infranet (di seguito con il termine DNS SPC² UQXN si indicherà il sistema DNS del generico soggetto interconnesso a QXN). Il Fornitore deve altresì tenere costantemente aggiornata la lista dei domini gestita dall'infrastruttura DNS QXN nell'Area informativa QXN di cui al requisito [R.236].
- [R.80] Il DNS QXN deve essere configurato per rispondere come DNS Autoritativo a tutte le query provenienti esclusivamente dai DNS SPC² UQXN e relative alla risoluzione dei nomi a dominio SPC². A tale scopo, i Name Server del DNS QXN devono essere configurati come DNS Slave rispetto ai DNS SPC² UQXN.
- [R.81] Il DNS QXN deve ricevere dai DNS SPC² UQXN le informazioni relative alle zone delle amministrazioni ad essi afferenti secondo un meccanismo di Zone Transfer (AXFR/IXFR) che potrà essere avviato dal DNS QXN:
- Periodicamente, in accordo con i parametri di configurazione di ciascuna zona;

- A seguito della ricezione di una direttiva DNS Notify inviata da un DNS SPC² UQXN in relazione alla modifica del contenuto di una zona in esso contenuta.
- [R.82] Il servizio DNS QXN deve permettere la configurazione di forwarding specifici per singoli domini.
- [R.83] Il servizio DNS QXN deve consentire la risoluzione dei nomi di dominio esterni allo spazio dei nomi della rete SPC² attraverso un collegamento Internet tra i DNS QXN ed i root server di Internet, utilizzando un accesso Internet opportunamente dimensionato e ridondato sia presso il nodo di Roma che presso il nodo di Milano. Tale collegamento Internet deve essere condiviso con quello utilizzato dal servizio NTP di cui al §1.10.
- [R.84] La connessione del DNS QXN verso Internet deve consentire esclusivamente il forwarding verso i root server Internet delle query ricevute dai DNS SPC² UQXN relative a richieste di risoluzione di nomi a dominio non SPC², qualora il DNS QXN non abbia in cache tale informazione.
- [R.85] Il DNS QXN non deve risolvere query DNS provenienti da Internet.
- [R.86] I sistemi di sicurezza perimetrale della QXN devono essere configurati a protezione del sistema DNS; in aggiunta il Fornitore deve prevedere opportune misure di filtraggio del traffico (es. ACL) e di sicurezza anche sui server costituenti il DNS QXN.
- [R.87] La soluzione implementativa proposta dal Fornitore deve presentare le seguenti caratteristiche:
- Alta affidabilità nei meccanismi di risoluzione dei nomi a dominio;
 - Alta affidabilità sui meccanismi di replica delle zone dai DNS SPC² UQXN;
 - Alta affidabilità delle componenti Hardware e di alimentazione.
- [R.88] Al fine di garantire il livello di disponibilità del servizio, il Fornitore deve implementare una configurazione che preveda la ridondanza geografica dei server DNS (o cluster di server). Tali apparati devono essere ubicati presso i siti QXN di Roma (NameX) e Milano (Mix).
- [R.89] Il servizio deve essere disponibile sia in IPv4 che in IPv6 e ciascuno dei server (o cluster server) DNS QXN di Roma e Milano deve essere raggiungibile da Infranet attraverso un indirizzo IP pubblico univoco appartenente allo spazio di indirizzamento definito in §1.3.

- [R.90] Gli indirizzi IP dei DNS QXN di Roma e Milano devono essere i forwarders dei DNS SPC² UQXN.
- [R.91] Per il management degli apparati e del servizio DNS QXN, il Fornitore deve prevedere dei collegamenti tra il proprio centro di gestione ed i nodi QXN di Roma e Milano. Al fine di proteggere il traffico di gestione remota degli apparati, tali collegamenti devono essere realizzati tramite tunnel IPSEC che saranno terminati:
- Lato QXN, sui firewall preposti alla sicurezza perimetrale di ciascuno dei due nodi QXN di Roma e Milano;
 - Lato Fornitore, su una coppia di firewall che il Fornitore deve prevedere.
- [R.92] Di seguito una figura che schematizza la logica di funzionamento del sistema DNS:

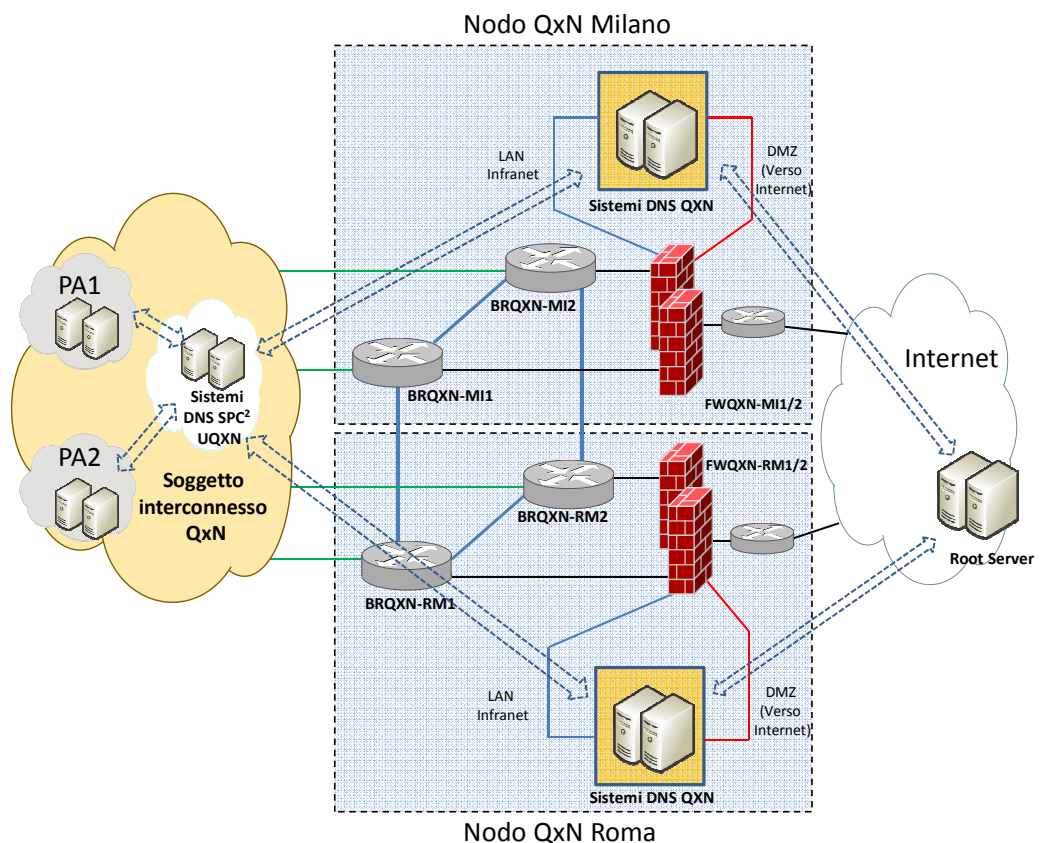


Figura 10

- [R.93] Il Fornitore deve progettare una soluzione che garantisca la massima affidabilità sulla connettività verso i root server Internet. A tal proposito, in entrambi i nodi DNS QXN di Roma e Milano, deve essere prevista una logica di

controllo sulla disponibilità dell'accesso Internet basata sull'invio periodico di query di test verso i root server. Qualora uno dei due nodi DNS QXN rilevi la mancata raggiungibilità di tutti i root server Internet, tale logica di controllo deve rendere non raggiungibile l'indirizzo IP con il quale il nodo DNS QXN viene contattato dai DNS SPC² UQXN. Questi ultimi, a loro volta, devono reinstradare automaticamente le query verso l'altro nodo DNS QXN. La logica di funzionamento dell'algoritmo di controllo è illustrata nella figura seguente per il nodo DNS QXN di Roma. Per il nodo di Milano la logica deve essere identica.

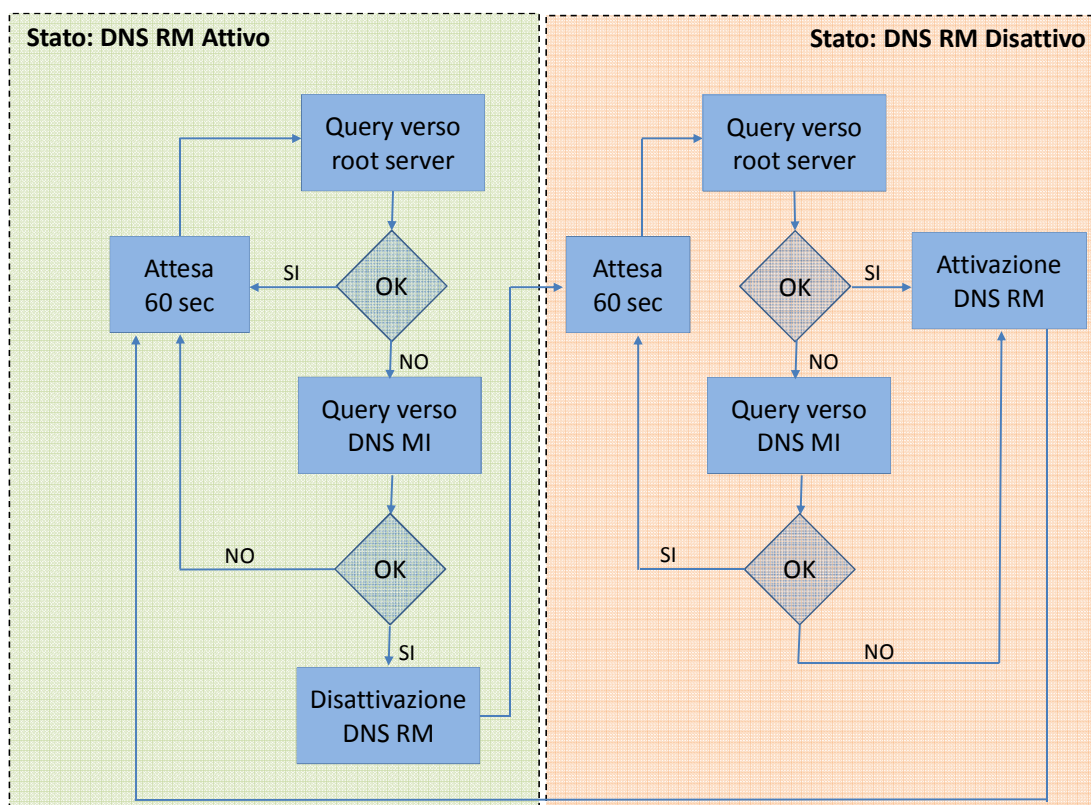


Figura 11

- [R.94] Il Fornitore deve definire e recepire all'interno del documento "Regole di Interconnessione QXN" di cui al [R.22] tutte le attività in capo ai soggetti che si interconnettono alla rete QXN propedeutiche alla corretta gestione del servizio DNS QXN.
- [R.95] Il Fornitore è tenuto al rispetto delle normative vigenti legate alla gestione di servizi DNS pubblici.

1.10 Servizio NTP

- [R.96] L'infrastruttura QXN deve erogare il servizio NTP v3 a tutti i soggetti interconnessi alla rete QXN (cfr. [R.13]) o partecipanti al SPC².
- [R.97] L'architettura QXN deve erogare il servizio NTP attraverso i BRqxn presenti sia nel nodo di Roma che di Milano. I BRQXN devono utilizzare una connessione Internet protetta per la sincronizzazione NTP in modalità autenticata con la sorgente di tempo ufficiale dell'Istituto Nazionale di Ricerca Metrologica (I.N.R.I.M.) (relazione Client Client). I BRqxn devono instaurare tra di loro una relazione peer-to-peer al fine di sopperire all'indisponibilità di uno dei collegamenti Internet presenti presso i nodi di Roma e Milano.
- [R.98] Il servizio NTP deve essere implementato per il tramite dell'infrastruttura gerarchica riportata nella figura seguente:

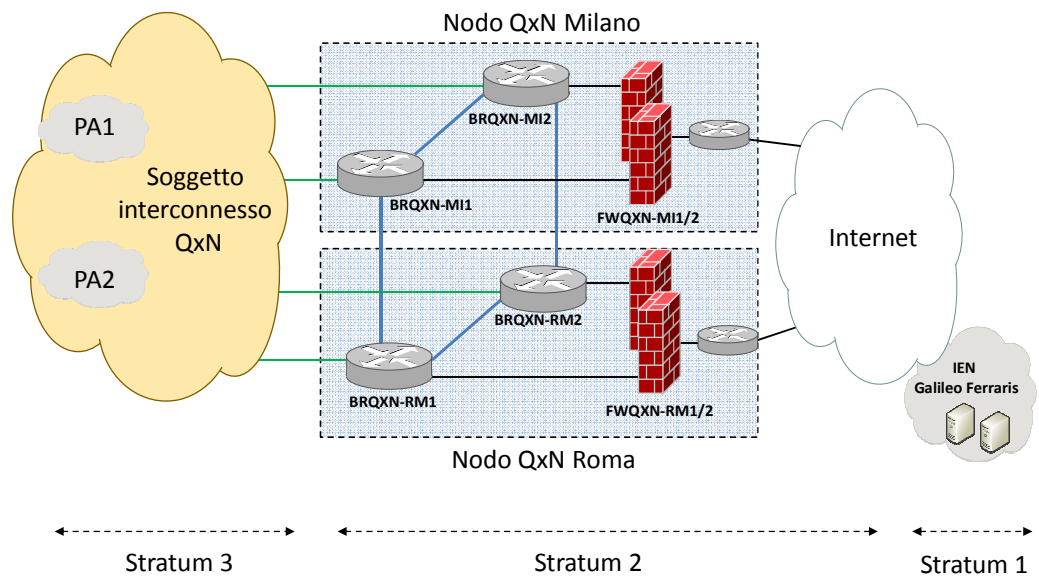


Figura 12

- [R.99] Il Fornitore deve progettare, realizzare e fornire gli apparati necessari ad un servizio NTP in alta affidabilità che consenta l'erogazione del servizio stesso per il tramite di un indirizzo IP primario posizionato presso il nodo di Roma ed un indirizzo IP secondario posizionato nel nodo di Milano.
- [R.100] Il Fornitore deve definire e recepire all'interno del documento "Regole di Interconnessione QXN" di cui al [R.22] tutte le attività in capo ai soggetti che si interconnettono alla rete QXN propedeutiche al corretto utilizzo del servizio NTP.

1.11 Circuiti di Collegamento Geografico

- [D.6] I circuiti di Collegamento geografico sono funzionali alla ridondanza del Profilo di Servizio “Interconnessione QXN OPA”, del servizio DNS, del servizio NTP e per il monitoring e la telegestione degli apparati.
- [R.101] I nodi QXN co-locati presso il Mix di Milano ed il Namex di Roma devono essere interconnessi con collegamenti ridondati di capacità almeno pari a 100 Mb/s e comunque adeguata alla quantità di traffico trasportato.
- [R.102] I collegamenti di cui al [R.101] devono essere realizzati mediante due circuiti geografici basati su tecnologia di trasporto SDH che soddisfino le seguenti condizioni:
- Completa diversificazione geografica dei percorsi ottici dei due circuiti;
 - Protezione sulla coda locale tramite anello ottico;
 - Completa diversificazione degli apparati trasmissivi di terminazione ADM dei due circuiti o, in subordine, attestazione dei due circuiti su schede di linea distinte dello stesso apparato trasmissivo;
 - Terminazione dei circuiti con interfaccia elettrica RJ45 o GBE ottica (Multimodale, SX).
- [R.103] L'apparato trasmissivo di terminazione ADM, su ciascun nodo QXN, deve essere completamente ridondato nelle sue parti comuni (matrice, alimentazione, schede di controllo). Ciascun router QXN deve essere collegato mediante connessione elettrica o ottica ad una scheda differente dell'ADM.
- [R.104] Deve essere possibile ampliare la banda di ciascun circuito, portandola fino ad 1 Gb/s, sempre utilizzando i medesimi apparati di trasporto e le medesime connessioni fisiche tra gli ADM ed i router QXN.
- [R.105] La decisione di procedere all'upgrade di banda dei due circuiti Roma-Milano deve essere presa in base alla seguente policy:
- a) Misurazione costante, su intervalli di osservazione T_i della durata di 10 minuti, dei valori della banda misurata sul circuito (B_i) nelle due direzioni di traffico ($B_{i\text{ RM} \rightarrow \text{MI}}$, $B_{i\text{ MI} \rightarrow \text{RM}}$).
 - b) Calcolo del picco giornaliero della banda misurata su ciascun circuito, definito come valore giornaliero di picco ($B_{\text{MAX}_{\text{day}_j}}$) dell'occupazione di banda sul circuito per ciascuna delle due direzioni di traffico nel

giorno j-esimo (massimo tra i valori dell'occupazione di banda misurati negli intervalli di osservazione T_i rilevati nell'arco delle 24 ore ($i=1..144$)).

$$B_MAX_{day_J\ RM \rightarrow MI} = \max B_{i\ RM \rightarrow MI} \quad (i=1.....144)$$

$$B_MAX_{day_J\ MI \rightarrow RM} = \max B_{i\ MI \rightarrow RM} \quad (i=1.....144)$$

- c) Calcolo della media dei valori giornalieri di picco ($B_MAX_{day_J}$) misurati su un periodo di un mese solare. Quindi, per ciascuno dei due circuiti Roma-Milano, si calcolano i seguenti valori:

$$B_{RM \rightarrow MI} = \text{avg} (B_MAX_{day_J\ RM \rightarrow MI}) \quad \text{per } j=1..30 \text{ (su un intervallo di 30 gg)}$$

$$B_{MI \rightarrow RM} = \text{avg} (B_MAX_{day_J\ MI \rightarrow RM}) \quad \text{per } j=1..30 \text{ (su un intervallo di 30 gg)}$$

- d) Con riferimento a ciascuno dei due circuiti, viene definita una soglia **Bs** pari al 50% della capacità trasmissiva massima configurata sul circuito (ad esempio per un circuito di 100Mbps abbiamo $Bs = 50$ Mbps).
- e) Attivazione della procedura di upgrade della banda nel momento in cui almeno uno tra i valori $B_{RM \rightarrow MI}$ e $B_{MI \rightarrow RM}$ supera la soglia **Bs**.
- f) Invio di esplicita comunicazione ad AgID del verificarsi della condizione di cui al comma precedente.
- g) Realizzazione dell'upgrade di velocità entro 60 giorni solari dal verificarsi della condizione di cui al precedente comma e).

L'ampliamento della capacità trasmissiva, su entrambi i circuiti, avviene con step minimi di 100 Mbps e fino ad un massimo di 1 Gbps per circuito secondo i seguenti tagli di banda: 200 Mbps, 300 Mbps, 600 Mbps, 1000 Mbps. Per velocità superiori ai 100 Mbps i circuiti dovranno essere terminati su interfaccia GBE ottica.

[R.106] Il Fornitore dovrà consegnare ad AgID la documentazione tecnica relativa alla realizzazione dei due circuiti, comprensiva di mappa di dettaglio dei percorsi fibra dei due circuiti, ubicazione degli apparati trasmissivi di terminazione dei circuiti presso i siti di Mix e Namex, schemi di cablaggio dei collegamenti rame e/o fibra tra apparati trasmissivi del Fornitore e gli apparati QXN all'interno dei siti Mix e Namex.

[R.107] Il Fornitore dovrà provvedere in autonomia a richiedere ed ottenere tutti i permessi necessari all'esecuzione delle opere connesse alla realizzazione del servizio, ivi comprese le autorizzazioni per la realizzazione dei cablaggi all'interno dei siti del Mix e del Namex. Su ciascuno dei due circuiti, il Fornitore dovrà assicurare i seguenti Livelli di Servizio:

- disponibilità servizio = 99,90 % su base annua;
- tempo di ripristino del disservizio: 4 ore dalla apertura del guasto nel 95% dei casi e 8 ore nel 100% dei casi.

1.12 Manutenzione

- [R.108] Ogni qualvolta sia necessario effettuare un intervento di manutenzione programmata sul dominio di competenza del Fornitore, questo deve informarne tutte le altre parti coinvolte (fornitori SPC², soggetti interconnessi alla rete QXN, AgID) specificando:
- Data ed ora prevista dell'intervento;
 - Durata prevista;
 - Descrizione del tipo di intervento da effettuare;
 - Eventuale interruzione del servizio erogato.
- [R.109] La comunicazione di cui al [R.108] deve essere effettuata via posta elettronica e confermata telefonicamente:
- Con almeno 5 giorni solari di anticipo in caso di manutenzione ordinaria ovvero di operazioni che possono essere pianificate con anticipo;
 - Con almeno 4 ore in caso di interventi di manutenzione straordinaria ovvero di operazioni che non possono essere pianificate con anticipo.
- [R.110] In ogni caso deve anche essere segnalata via posta elettronica e confermata telefonicamente la chiusura delle operazioni, specificando l'ora in cui l'intervento è stato portato a termine ed eventuali anomalie/disservizi riscontrati durante l'intervento.
- [R.111] Gestione upgrade del SW: gli avanzamenti di release, ove possibile, non devono 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.
- [R.112] Le procedure che regolano le attività di manutenzione devono essere recepite all'interno del documento "Regole di Interconnessione QXN" di cui al [R.22].

1.13 Sistemi di gestione e misura dei livelli di servizio

- [R.113] Il Fornitore deve realizzare un sistema che consenta la gestione *in-band* di tutti gli apparati utilizzati all'interno della rete QXN e, al fine di far fronte a situazioni critiche di troubleshooting ed effettuare operazione di manutenzione straordinaria, prevedere in entrambi i nodi di Roma e Milano un terminal server che consenta l'accesso *out-of-band* ai dispositivi di rete per il tramite della porta console di ciascun apparato.

- [R.114] Gli apparati per la gestione *out-of-band* di cui al requisito [R.113] devono essere equivalenti o superiori a quelli descritti all'interno del paragrafo "2.2 Terminal server per la gestione OOB" del documento "Specifica di Realizzazione del servizio InterConnessione QXN" di cui al [D.4].
- [R.115] Al fine di monitorare i livelli di servizio previsti per le due tipologie di traffico OPA e OPO, l'infrastruttura QXN deve essere dotata di un sistema di monitoraggio delle prestazioni di rete funzionalmente equivalente a quello descritto all'interno del documento "Specifica di Controllo InterConnessione QXN" di cui al [D.4].
- [R.116] Il sistema di monitoraggio deve verificare costantemente il rispetto dei parametri definiti nell'appendice "SLA e Penali".
- [R.117] Ciascuna delle sonde fisiche per la misurazione degli SLA può svolgere contemporaneamente la funzione logica di *querier* e *responder* e deve essere equivalente o superiore a quella descritta all'interno del paragrafo "2.4 Sonde per la misurazione degli SLA" del documento "Specifica di Realizzazione del servizio InterConnessione QXN" di cui al [D.4].

2 Servizi per l'Interoperabilità delle Applicazioni (SIA)

[R.118] I Servizi per l'Interoperabilità delle Applicazioni comprendono:

- a **Servizio di Certificazione (SPKI):** servizio di PKI finalizzato all'emissione di certificati PEC e di Cooperazione Applicativa;
- b **Servizio di Gestione del Repertorio Nazionale dei Dati Territoriali (RNDT):** istituito con l'art. 59 del CAD è il catalogo nazionale dei metadati riguardanti i dati territoriali - e relativi servizi - disponibili presso le Pubbliche Amministrazioni, deputato a garantire l'erogazione del servizio di ricerca a livello nazionale e comunitario;
- c **Servizio Indice della Pubblica Amministrazione (IPA):** istituito con il DPCM del 31 ottobre 2000 recante le "Regole tecniche per il protocollo informatico, costituisce l'archivio ufficiale contenente i riferimenti organizzativi, telematici e toponomastici degli Enti Pubblici. L'articolo 57 bis del decreto legislativo 7 marzo 2005 n. 82 (Codice dell'Amministrazione Digitale), pone in capo agli Enti la responsabilità dei dati pubblicati e il loro costante aggiornamento. L'IPA espone sia un'interfaccia web sia un'interfaccia applicativa, tramite protocollo LDAP; i contenuti sono pubblicati in formato Open Data;
- d **Servizio Indice dei Gestori PEC (IGPEC):** la normativa affida ad AgID il ruolo di vigilanza e controllo sull'operato dei gestori PEC. In tale contesto l'Agenzia gestisce l'elenco pubblico dei gestori di posta elettronica certificata. In tale ambito accoglie e valuta le domande presentate dai soggetti che si candidano al ruolo di gestori di posta elettronica certificata, decretandone l'iscrizione nell'apposito elenco o respingendone la domanda, per carenze di requisiti. Ai soggetti iscritti l'Agenzia fornisce i certificati per la firma elettronica delle ricevute e per l'accesso e l'aggiornamento della struttura tecnica che costituisce l'insieme dei domini di posta elettronica certificata, definita indice dei gestori PEC (IGPEC). I gestori devono presentare all'Agenzia eventuali modifiche in ordine all'assetto societario, alle caratteristiche del servizio, alle procedure adottate, con particolare riguardo agli aspetti di continuità, di funzionamento e di sicurezza.

[R.119] I servizi di cui al requisito [R.118]

- Lettera a), devono essere erogati esclusivamente verso le Pubbliche Amministrazioni e verso i soggetti sussidiari (nelle modalità previste dal DPCM. 1° aprile 2008 recante le "Regole Tecniche per i servizi di connettività e sicurezza SPC")
- Lettere b) e c), devono essere accessibili in consultazione all'utente generico del World Wide Web (WWW) e, tramite

autenticazione, ai soggetti titolati (Pubbliche Amministrazioni, Società interamente partecipate da Enti Pubblici o con prevalente capitale pubblico, Gestori di pubblici servizi) all'accreditamento, l'inserimento, la modifica e la cancellazione dei dati

- Lettera d), deve essere accessibile su internet, tramite autenticazione, unicamente ai soggetti abilitati (gestori PEC e l'Agenzia per l'Italia Digitale).

[R.120] Il Fornitore deve progettare la propria soluzione facendo riferimento a quanto previsto nei documenti allegati per gli specifici servizi richiamati nei successivi paragrafi e relativi ai sistemi attualmente in esercizio. Il Fornitore potrà proporre modalità di dispiegamento alternative anche basate su sistemi virtualizzati. Le modalità proposte dovranno comunque garantire equivalenti caratteristiche di affidabilità e sicurezza.

[R.121] Il Fornitore deve rendere disponibile un servizio DNS con il quale esporre/gestire le zone e i relativi host associati ai servizi del presente capitolo. A seconda delle caratteristiche del singolo servizio le zone devono essere pubblicate o sulla Rete Internet/Infranet o sulla Rete Infranet.

2.1 Servizio di Certificazione (SPKI)

[R.122] Il servizio è finalizzato alla predisposizione e alla gestione di un'infrastruttura PKI finalizzata all'emissione di certificati X509v3 da utilizzarsi nei seguenti ambiti:

- a. Posta Elettronica Certificata (PEC)
- b. Cooperazione Applicativa SPCoop

Certificazione nell'ambito della PEC

[R.123] Il servizio deve realizzare una PKI pubblica che emetta certificati destinati ai Gestori PEC.

[R.124] Il Fornitore deve acquisire, e utilizzare nella PKI che realizza, un certificato root intestato all'Agenzia per l'Italia Digitale rilasciato da una delle Certification Authority (CA) riconosciute automaticamente dai web browser più diffusi.

[R.125] La PKI dovrà garantire l'emissione e la gestione di certificati per:

- Chiavi pubbliche per la firma delle ricevute PEC;
- Chiavi pubbliche di autenticazione del client SSL per server;

- Chiavi pubbliche per Web Server.
- I certificati da emettere saranno dei certificati server con i profili definiti nel “Manuale Operativo per il servizio ‘DigitPA-CA1’ – Certificate Practice Statement” (cfr. MO_DigitPA-CA1_v2.1_0.pdf, in appendice 3).

[R.126] Il numero massimo complessivo di certificati da emettere è pari a 120 annui; l’Agenzia per l’Italia Digitale si riserva la possibilità, previa tempestiva comunicazione al Fornitore, di elevare tale limite massimo.

Certificazione nell’ambito della Cooperazione applicativa SPCoop

[R.127] Il servizio deve realizzare una PKI privata ad uso interno al circuito SPC² sulla base di un certificato *self-signed* generato allo startup del servizio o fornito dall’Agenzia per l’Italia Digitale.

[R.128] Il servizio deve provvedere all’emissione di certificati per le Porte di Dominio qualificate sulla base di CSR fornite dalle Amministrazioni che richiedono la qualificazione previa verifica di correttezza delle richieste.

[R.129] Il Fornitore deve garantire l’emissione di certificati con profili definiti nel documento “Manuale Operativo per il servizio ‘DigitPA Certificati Server SPCoop’ – Certificate Practice Statement” (cfr. MO_DigitPA_CertificatServerSPCoop_Ver2 0_REV_1 7.pdf, in appendice 3).

2.2 Servizio di Gestione del Repertorio Nazionale dei Dati Territoriali (RNDT)

[R.130] Il servizio di Gestione del Repertorio Nazionale dei Dati Territoriali comprende:

- La progettazione, realizzazione e messa in esercizio di una nuova versione del portale web e dell'applicazione del RNDT per la gestione dei metadati relativi ai dati territoriali - comprensivo dei relativi servizi - mediante la personalizzazione e/o estensione di un prodotto o pacchetto completo già esistente e realizzato con tecnologie open-source o reso disponibile in riuso nell'ambito di INSPIRE;
- Porting dei dati facenti parte della base dati relativa alla attuale versione del portale web e dell'applicazione del RNDT;

- La gestione ed il monitoraggio del servizio, inclusa la manutenzione e la gestione sistemistica dell'ambiente di produzione e di pubblicazione su web della nuova versione del portale del RNDT;
- Le attività finalizzate alla Gestione operativa e amministrazione della nuova versione del portale del RNDT (riservata ad AgID);
- La manutenzione correttiva, adeguativa ed evolutiva del portale del RNDT.

[R.131] Il Repertorio Nazionale dei Dati Territoriali (RNDT) è il catalogo di metadati relativo ai dati territoriali - e ai servizi ad essi connessi - disponibili presso le pubbliche amministrazioni. Come previsto dall'art. 59 del CAD, AgID ha il compito di implementare e gestire il Repertorio Nazionale dei Dati Territoriali, già individuato come base di dati di interesse nazionale dal successivo art. 60 del CAD. Attraverso i metadati in esso contenuti, il RNDT consente di conoscere ufficialmente, per i suddetti dati, una serie di informazioni controllate, di cui è certa la provenienza e l'affidabilità e di cui l'amministrazione titolare è pienamente responsabile. L'obiettivo dell'attività è quello di sviluppare una nuova versione operativa del RNDT, cioè un portale basato sul web che deve supportare due macro-processi fondamentali:

- a) Raccolta dei metadati predisposti e inviati dalle pubbliche amministrazioni abilitate;
- b) Ricerca e consultazione dei metadati raccolti da parte di tutti i soggetti interessati, sia pubblici che privati.

[R.132] Il Fornitore deve garantire che la nuova piattaforma per l'erogazione del servizio RNDT:

- Fornisca uno specifico punto di accesso multilingue ai servizi di ricerca e visualizzazione (dei metadati contenuti nel catalogo) contemplati dalla direttiva INSPIRE e relative regole di implementazione. Per quanto riguarda il multilinguismo, nella fase iniziale sarà sufficiente garantire la localizzazione in italiano e inglese delle interfacce che permetteranno l'accesso e l'utilizzo dei servizi di ricerca e visualizzazione, ma dovrà essere possibile per AgID, in modo flessibile e configurabile, aggiungere il supporto ad ulteriori lingue, in particolare a quelle facenti parte dell'Unione Europea;

- Fornisca agli utenti un'interfaccia di facile utilizzo che permetta di accedere, in modo agevole, alle risorse e ai servizi esposti, sia come utente amministratore del portale (AgID), sia come utente abilitato all'invio dei metadati (pubbliche amministrazioni), che infine come utente generico per la semplice consultazione dei metadati raccolti dal RNDT;
- Permetta ai soggetti abilitati (pubbliche amministrazioni) l'alimentazione del RNDT attraverso le diverse modalità previste, sia attraverso GUI web-based che attraverso web-service. Per quanto riguarda l'alimentazione in modalità GUI web-based, deve essere possibile per le pubbliche amministrazioni sia l'alimentazione tramite file XML precompilato, che l'utilizzo di un editor on-line, facente parte del portale del RNDT e in grado di generare il file XML da utilizzare per l'alimentazione del portale stesso. Per quanto riguarda l'alimentazione del RNDT tramite web-service, dovrà essere resa disponibile sia secondo quanto previsto dagli standard OGC per i servizi CSW (*harvesting*) e dalla Direttiva INSPIRE per i servizi di Discovery, sia in modalità di cooperazione applicativa fra servizi secondo quanto stabilito dall'art. 20 del DPCM 1 aprile 2008 recante "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività previste dall'articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n. 82, recante il «Codice dell'amministrazione digitale»";
- Sia modulare, scalabile e basata su standard aperti, partendo comunque da un prodotto già esistente che utilizzi tecnologie open source;
- Sia configurabile e possa integrarsi dal punto di vista grafico con gli altri siti e portali istituzionali gestiti dall'Agenzia per l'Italia Digitale
- Sia debitamente documentata;

- Sia corredata da processi definiti per i successivi aggiornamenti e relativa manutenzione.

[R.133] Il Fornitore deve garantire che la nuova versione del RNDT sia conforme alle seguenti normative:

- Decreto 10 novembre 2011 (pubblicato sulla G.U. n. 48 del 27 febbraio 2012 – Supplemento ordinario n. 37) "Regole tecniche per la definizione del contenuto del Repertorio Nazionale dei Dati Territoriali nonché delle modalità di prima costituzione e di aggiornamento dello stesso";
- Decreto Legislativo 27 gennaio 2010 n.32 recante "Attuazione della Direttiva 2007/2/CE, che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE)";
- Regolamento CE n. 1205/2008 della Commissione del 3 dicembre 2008, e s.m.i., recante attuazione della direttiva INSPIRE per quanto riguarda i metadati;
- Regolamento CE n. 976/2009 della Commissione del 19 ottobre 2009, e s.m.i., recante attuazione della direttiva INSPIRE per quanto riguarda i servizi di rete di ricerca e visualizzazione;
- Regolamento UE n. 1089/2010 della Commissione del 23 novembre 2010, e s.m.i., recante attuazione della direttiva INSPIRE per quanto riguarda l'interoperabilità;
- Legge n. 4/2004 (cd legge Stanca) e Decreto MIUR del 20/03/2013 pubblicato sulla GU Serie Generale n.217 del 16-9-2013.

[R.134] Il Fornitore deve altresì garantire che la nuova versione del RNDT sia conforme ai seguenti standard e specifiche tecniche nazionali e internazionali di riferimento:

- UNI EN ISO 19115:2005, Geographic Information – Metadata;
- UNI EN ISO 19119:2006, Geographic Information – Services;
- ISO TS 19139:2007 – Geographic Information - Metadata – XML Schema Implementation;

- OGC, OpenGIS Catalogue Services Specification 2.0.2 – ISO Metadata Application Profile, version 1.0.0, 2007;
- INSPIRE Metadata Implementing Rules: Technical Guidelines based on EN ISO 19115 and EN ISO 19119;
- Technical Guidance for the implementation of INSPIRE Discovery Services;
- Le guide operative in appendice 4:
 - Manuale RNDT - 2. Guida operativa per la compilazione dei metadati RNDT sui dati in coerenza con il Regolamento INSPIRE (RNDT_guida_operativa_dati_v2.0_20140725.pdf);
 - Manuale RNDT - 3. Guida operativa per la compilazione dei metadati RNDT sui servizi in coerenza con il Regolamento INSPIRE (RNDT_guida_operativa_servizi_v2.0_20140725.pdf);
 - Manuale RNDT - 4. Guida operativa per la compilazione dei metadati RNDT sulle nuove acquisizioni di dati (RNDT_guida_operativa_nuove_acquisizioni_v2.0_20140725.pdf)
 - Manuale RNDT - 5. Guida operativa per la compilazione dei metadati RNDT sui dati raster in coerenza con il Regolamento INSPIRE (RNDT_guida_operativa_datiraster_v2.0_20140725.pdf);
 - Manuale RNDT – Errata Corrige (Manuale_RNDT_errata_corrige.pdf).

[R.135] Il Fornitore deve garantire, per la nuova versione del RNDT, l'implementazione di un set minimo di funzionalità e/o classi, così come descritte in tabella:

Nome	Descrizione	Dati	
		Input	Output
Pubblicazione di informazioni, news e documenti	Consente all'utente amministratore (AgID) di pubblicare informazioni, news e documenti digitali relativi al	Informazioni in forma testuale eventualmente corredate da	Scheda HTML contenente le informazioni e le immagini

digitali	RNDT e di renderli pubblicamente accessibili sul web. La funzionalità da garantire è assimilabile a quella normalmente fornita da un sistema CMS (Content Management System).	immagini e documenti digitali (doc, pdf, odt, ...) inserite dall'utente amministratore del portale	inserite (informazioni e news), link per il download dei documenti digitali
Ricerca semplice	Consente di ricercare nel Catalogo i metadati attraverso l'impostazione di un set minimo di criteri di ricerca (sia alfanumerici che spaziali)	Dati alfanumerici (parametri di ricerca) o spaziali	Scheda HTML con l'elenco dei set di metadati
Ricerca avanzata	Consente di ricercare nel Catalogo i metadati attraverso l'impostazione di un set più dettagliato di criteri di ricerca (sia alfanumerici che spaziali)	Dati alfanumerici (parametri di ricerca) o spaziali	Scheda HTML con l'elenco dei set di metadati
Ricerca accessibile	Consente di ricercare nel Catalogo, in modo accessibile, i metadati attraverso l'impostazione di un set di criteri di ricerca prettamente alfanumerici.	Dati alfanumerici (parametri di ricerca)	Scheda HTML con l'elenco dei set di metadati
Guida On-Line	Fornisce una guida on-line per la consultazione dei metadati presenti nel RNDT, l'utilizzo dei moduli di ricerca da parte dell'utente generico e dei servizi riservati alla PA.	----	Scheda HTML con istruzioni per la consultazione dei metadati e l'utilizzo dei moduli di ricerca
Visualizzazione dettaglio metadati	Consente di visualizzare, in una scheda HTML, i metadati relativi ad un dataset/servizio di interesse	----	Scheda HTML con l'elenco dei metadati relativi ad un dataset/servizio
Navigatore geografico	Web- GIS che consente di interagire con la mappa e i livelli informativi presenti allo scopo di	----	Mappa

	<p>ricercare, attraverso criteri di ricerca geografici, i metadati di interesse, visualizzarli e localizzarli. Le funzioni presenti sono le seguenti:</p> <ul style="list-style-type: none"> • Funzione di <i>identify</i> (visualizza gli attributi dei layer vettoriali rappresentati nella mappa). • Funzione di <i>pan</i> (sposta la porzione della mappa visualizzata) • Funzione di <i>zoom out</i> (riduce la mappa visualizzata) • Funzione di <i>zoom in</i> (ingrandisce la mappa visualizzata) • Funzione di <i>zoom su area selezionata</i> (ingrandisce l'area selezionata) • Funzione di <i>zoom full extent</i> (visualizza l'intera mappa) • Funzione di <i>map overview</i> (evidenzia sull'Italia, l'area visualizzata) • Barra degli <i>zoom a scala predefinita</i>. Il livello di zoom corrente è segnato in rosso • Guida on-line 		
Download file XML	Consente di scaricare i file XML contenente i metadati relativi a dataset/servizi di interesse in diversi profili.	----	File XML dei metadati
Validazione XML	Consente di validare i file XML contenente i metadati rispetto agli schemi XSD di riferimento e alle regole tecniche del RNDT.	File XML contenente i metadati	File XML contenente il log di validazione comprensivo di eventuali segnalazioni di errore

Upload file XML	Consente di caricare i file XML nel DB, contestualmente alla validazione degli stessi.	File XML	File XML contenente il log di caricamento
Editor metadati	Consente di compilare i metadati attraverso form alfanumeriche, salvare e/o cancellare la sessione di lavoro, visualizzare, validare, trasmettere ed esportare il file XML generato.	Dati alfanumerici	Scheda HTML/File XML
Lista documenti	Visualizza l'elenco dei documenti (file XML) trasmessi	----	Elenco documenti trasmessi
Ricerca documenti	Consente di ricercare i documenti (file XML) trasmessi attraverso l'impostazione di un set di criteri di ricerca	Dati alfanumerici (parametri di ricerca)	Elenco documenti (file XML)
Gestione Enti	Consente di gestire tutta l'anagrafica relativa alle Amministrazioni accreditate che, in un dato contesto, utilizzano l'Oggetto. Funzione riservata all'Amministratore dell'Oggetto.	Dati alfanumerici	Scheda HTML contenente le informazioni sugli Enti
Gestione Utenti	Consente di gestire tutta l'anagrafica degli utenti appartenenti alle Amministrazioni accreditate che, in un dato contesto, utilizzano l'Oggetto. Funzione riservata all'Amministratore dell'Oggetto.	Dati alfanumerici	Scheda HTML contenente le informazioni sugli utenti
Trasmissione file XML	Consente di inviare al gestore dell'Oggetto i file XML generati e validati dall'editor.		
Login	Consente di accedere all'area riservata di gestione dei metadati	Credenziali di accesso	Eventuali messaggi di errore
Logout	Consente di terminare una sessione di lavoro nell'area riservata di gestione dei		

	metadati.		
Sincronizzazione e pubblicazione	Consente di copiare nello schema DB di pubblicazione i dati caricati dalle singole Amministrazioni nello schema DB di staging (attraverso il file XML) per renderli disponibili in consultazione. Funzione riservata all'Amministratore dell'Oggetto.		
Monitoraggio	Consente di monitorare gli accessi e le operazioni effettuate dagli utenti. Funzione riservata all'Amministratore dell'Oggetto.		
Modifica stato documento	Consente di cambiare lo "stato" del documento trasmesso (file XML) in corrispondenza di parametri predefiniti. Funzione riservata all'Amministratore dell'Oggetto.		

Tabella 3

[R.136] Il Fornitore deve garantire che, la nuova versione del RNDT, offra e supporti i servizi e le procedure descritti in tabella:

Nome servizio	Descrizione sintetica	Destinatari del servizio
Alimentazione del catalogo - Editor	Strumento per l'acquisizione e l'aggiornamento dei metadati attraverso la compilazione di form alfanumeriche guidate e conformi al modello di metadati del RNDT come definito dal DM 10-11-2011. L'editor crea automaticamente un file XML conforme agli schemi XSD di riferimento.	<ul style="list-style-type: none"> – Personale Agenzia Italia Digitale – Altre PA
Alimentazione del catalogo - Upload file XML	Servizio che permette di trasmettere, per la successiva pubblicazione, i file XML di metadati, previa verifica di conformità agli	<ul style="list-style-type: none"> – Personale Agenzia Italia Digitale – Altre PA

	schemi XSD e alle indicazioni contenute nel DM.	
Alimentazione del catalogo - Web Service conforme standard SPC	<p>Servizio che permette di trasmettere, per la successiva pubblicazione, i file XML di metadati, previa verifica di conformità agli schemi XSD e alle indicazioni contenute nel DM.</p> <p>La trasmissione avviene mediante l'utilizzo di WebService conforme agli standard SPC</p>	<ul style="list-style-type: none"> – Personale Agenzia Italia Digitale – Altre PA
Alimentazione del catalogo - Web Service conforme standard OGC - CSW (Harvesting)	<p>Servizio che permette di raccogliere, per la successiva pubblicazione, i file XML di metadati, previa verifica di conformità agli schemi XSD e alle indicazioni contenute nel DM.</p> <p>La raccolta dei file XML avviene mediante l'utilizzo di Web Service conforme agli standard OGC - CSW</p>	<ul style="list-style-type: none"> – Personale Agenzia Italia Digitale – Altre PA
Validazione dei dati inseriti nel catalogo	Servizio che verifica la conformità dei file XML agli schemi XSD e alle regole tecniche del RNDT.	<ul style="list-style-type: none"> – Personale Agenzia Italia Digitale – Altre PA
Pubblicazione on-line dei dati inseriti	Servizio che rende disponibili i dati caricati e validati attraverso il portale web del RNDT.	<ul style="list-style-type: none"> – Personale Agenzia Italia Digitale
Ricerca nel catalogo – portale	Servizio che permette di ricercare attraverso l'impostazione di criteri i metadati pubblicati nel portale	<ul style="list-style-type: none"> – Cittadini – Imprese – Liberi professionisti – Personale Agenzia Italia Digitale – Altre PA
Ricerca nel catalogo - Web Service conforme standard OGC - CSW	Servizio che permette di ricercare attraverso l'impostazione di criteri i metadati pubblicati nel portale. Il servizio viene attivato mediante Web Service conforme agli standard OGC - CSW. Il suddetto CSW dovrà ottenere la certificazione di conformità rilasciata da OGC.	<ul style="list-style-type: none"> – Cittadini – Imprese – Liberi professionisti – Personale Agenzia Italia Digitale – Altre PA

Autenticazione	Consente l'accreditamento degli Enti e relativi utenti	<ul style="list-style-type: none"> – Personale Agenzia Italia Digitale – Altre PA
----------------	--	---

Tabella 4

[R.137] Il Fornitore deve prevedere l'implementazione di almeno tutte le funzionalità presenti nella versione del Repertorio attualmente in produzione.

[R.138] Il Fornitore dovrà produrre, in accordo e di concerto con AgID, un documento che descriva nel dettaglio le specifiche funzionali della nuova versione del RNDT. Per la redazione del suddetto documento il Fornitore dovrà far riferimento alle funzionalità, ai servizi e alla procedure che afferiscono al RNDT e che sono descritte nel presente capitolo o che sono già implementate nella versione del RNDT attualmente operativa. Il documento dovrà essere redatto e consegnato dal Fornitore entro 45 giorni solari dalla stipula del contratto, nell'ambito del Progetto esecutivo di cui al paragrafo 5.1. L'approvazione del documento da parte di AgID sarà propedeutica all'avvio di tutte le fasi successive dell'attività.

[R.139] Il Fornitore deve consegnare ad AgID tutta la documentazione e i sorgenti relativi alla nuova versione del RNDT; in particolare devono essere opportunamente documentati:

- Architettura di sistema;
- Documentazione tecnica di dettaglio relativa alle classi e ai componenti software implementati;
- Codice sorgente dell'applicativo;
- Procedura di installazione e configurazione dell'applicativo.

Devono inoltre essere predisposti i seguenti documenti:

- Manuale di gestione operativa e di amministrazione del sistema applicativo (destinato ad AgID);
- Manuale utente (destinato alle pubbliche amministrazioni abilitate al caricamento dei metadati nel RNDT).

[R.140] Il Fornitore deve garantire che il software realizzato sia di completa proprietà di AgID e dovrà essere reso disponibile con licenza *open-source* e in *riuso gratuito*.

[R.141] Il Fornitore deve prevedere l'esercizio della nuova versione della piattaforma RNDT presso il proprio data center, realizzando l'ambiente di produzione con tutti i nodi necessari per il corretto funzionamento del portale, del software

applicativo e dei relativi servizi che, secondo le diverse modalità previste, sono finalizzati alla corretta esecuzione dei macro-processi indicati al paragrafo precedente.

- [R.142] La messa in esercizio del nuovo Repertorio Nazionale dei Dati Territoriali deve essere preceduta dal porting di tutti i dati che, a quella data, saranno presenti in produzione nel Database del Repertorio. Per la realizzazione delle attività di migrazione dei dati AgID fornirà tutto il supporto e le informazioni necessari al corretto completamento dell'attività.
- [R.143] La gestione operativa del Repertorio Nazionale dei Dati Territoriali sarà effettuata direttamente da AgID.
- [R.144] Il Fornitore dovrà realizzare un apposito cruscotto operativo attraverso il quale sia possibile dare corso alle necessarie funzioni di gestione, anche attraverso l'implementazione e/o l'esecuzione di query del DB; si elencano qui le principali:
- Gestione anagrafica utenti (almeno creazione, modifica, eliminazione degli utenti);
 - Gestione anagrafica enti (almeno creazione, modifica, eliminazione degli enti);
 - Gestione dati XML trasmessi dagli utenti;
 - Gestione sessioni editor XML on-line del RNDT, utilizzate dalle amministrazioni per compilare i metadati da inviare;
 - Monitoraggio accessi e operazioni effettuati dagli utenti;
 - Creazione/esportazione report statistici;
 - Gestione operativa dei servizi CSW/SPC (in particolare per quanto riguarda l'utilizzo e la gestione degli end-point esterni utilizzati dalle amministrazioni abilitate per inviare i metadati in formato XML al RNDT tramite web-service).
- [R.145] Qualora esplicitamente richiesto da AgID il Fornitore deve impegnarsi ad erogare un corso di formazione, in modalità on-site, della durata di 2 giorni, per un max di 10 partecipanti, presso la sede di AgID per il personale addetto alla gestione operativa e all'amministrazione della nuova versione del RNDT.
- [R.146] Il Fornitore, nell'ambito della gestione del servizio, deve garantire una adeguata gestione delle versioni del software e mantenere allineata:

- La documentazione
- La lista dei malfunzionamenti rilevati con l'indicazione delle relative risoluzioni.

[R.147] Su richiesta dell'Amministrazione, il Fornitore deve garantire i **servizi di sviluppo** necessari alla manutenzione correttiva, adeguativa ed evolutiva del Servizio di Gestione del RNDT secondo quanto previsto nel §4.5; le attività previste potranno essere volte:

- *(Manutenzione correttiva)* alla correzione di eventuali malfunzionamenti dell'applicazione
- *(Manutenzione adeguativa)* all'adeguamento delle funzionalità del sistema resi necessari ad esempio a seguito di modifiche normative, evoluzione delle tecnologie e dei prodotti correlati
- *(Manutenzione evolutiva)* all'aggiunta di nuove funzionalità attualmente non previste.

[R.148] Le attività di manutenzione adeguativa ed evolutiva di cui al paragrafo 4.5 dovranno essere svolte con l'impiego delle figure professionali di cui al [R.150] e nei limiti indicati alla seguente tabella:

FIGURA PROFESSIONALE	TARIFFA MASSIMA	GG/U STIMATI
Analista Programmatore	350 €	50
Programmatore	250 €	270
Totale	85.000 €	

[R.149] L'importo totale di € 85.000,00 (IVA esclusa) rappresenta il limite massimo spendibile nei 60 mesi di durata contrattuale; di conseguenza, a tariffe unitarie più basse offerte potrebbe corrispondere una maggiore richiesta di attività da parte dell'Agenzia per l'Italia Digitale.

[R.150] Le figure professionali da impiegare nelle attività di sviluppo adeguativa ed evolutiva dovranno corrispondere ai seguenti profili professionali minimi:

Analista Programmatore

Titolo di Studio	Diploma di perito informatico o cultura superiore in ambito tecnico-scientifico
Esperienze Lavorative	<ul style="list-style-type: none"> • Anzianità minima di 4 anni come programmatore e di 1 anno nella funzione • Coordinamento di piccoli gruppi di lavoro • Verifica della corretta applicazione di metodi e standard • Sviluppo di analisi tecnica di media complessità • Documentazione di procedure • Programmazione strutturata, in ambiente client-server, Web e SOA • Preparazione casi di test ed esecuzione di test • Predisposizione di script per il testing automatico con i principali prodotti per il testing automatico • Partecipazione a gruppi di progetto di medie/grandi dimensioni • Tecnologie emergenti • Metodologie di analisi e disegno di prodotti SW • Installazione e personalizzazione di sistemi anche complessi • Progettazione ed integrazione di sistemi • Tecniche di programmazione strutturata • Pacchetti software relativi al progetto • Esperienza di lavoro nel campo dei sistemi informativi territoriali e delle infrastrutture dei dati territoriali
Conoscenze	<ul style="list-style-type: none"> • Metodologie di disegno di prodotti software • DBMS relazionali, SQL • Strumenti di modellazione dati • Tecniche di programmazione Object Oriented • Strumenti per il cleaning e la qualità dei dati • Strumenti di ETL • Web designer (grafico) • Ottima conoscenza di tecniche di configuration management del software

Programmatore	
Titolo di Studio	Diploma di perito informatico o cultura superiore in ambito tecnico-scientifico
Esperienze Lavorative	<ul style="list-style-type: none"> • Anzianità minima di 3 anni come programmatore • Sviluppo di analisi tecnica di bassa complessità • Progettazione ed Esecuzione di test • Preparazione di documentazione di programmi • Partecipazione alla stesura di specifiche tecniche • Partecipazione a gruppi di progetto di medie dimensioni • Programmazione in ambiente client-server, Web e SOA • Metodologie di analisi, disegno di prodotti SW • Installazione e personalizzazione di sistemi anche complessi • Progettazione ed integrazione di sistemi • Strumenti per la codifica dei programmi • Tecniche di programmazione strutturata • Esperienza di lavoro nel campo dei sistemi informativi territoriali e delle infrastrutture dei dati territoriali

Conoscenze	<ul style="list-style-type: none"> • Ha una completa autonomia nello sviluppo, nella preparazione ed esecuzione di casi di test di unità, nella preparazione di documentazione di programmi, nella stesura di specifiche tecniche. • Strumenti per la codifica dei programmi • DBMS relazionali, SQL • Tecniche di programmazione
-------------------	---

2.3 Servizio Indice della Pubblica Amministrazione (IPA)

[R.151] Il servizio IPA comprende:

- La presa in carico del servizio garantendo senza soluzione di continuità la disponibilità di tutte le funzionalità fino al termine della fase di migrazione
- La progettazione, realizzazione e messa in esercizio del nuovo ambiente di produzione dedicato del servizio e dell'ambiente dedicato al collaudo/pre-esercizio secondo l'architettura prevista al requisito [R.152],
- L'erogazione del Service Desk IPA descritto al requisito [R.164], per il supporto all'utenza, anche telefonico, sia a fini informativi sia per la corretta esecuzione di tutti i processi applicativi legati alle richieste dell'utenza stessa (ad es. accreditamento di un ente), comprese le componenti tecnologiche a supporto e relativi strumenti software;
- La progettazione e realizzazione della fase di migrazione del sistema nel rispetto del requisito [R.152];
- La gestione ed il monitoraggio del servizio, inclusa la manutenzione e la gestione sistemistica dell'ambiente di produzione;
- La manutenzione correttiva, adeguativa ed evolutiva di tutte le componenti del servizio;
- L'esecuzione periodica di stress-test volti a rilevare e misurare le prestazioni del sistema sotto particolari condizioni di carico.

[R.152] Il Fornitore deve acquisire tutte le informazioni necessarie per l'erogazione del servizio dai documenti in appendice 5, che specificano le finalità, le funzionalità e l'architettura dell'IPA:

- Infrastruttura IPA - Documentazione tecnica (InfrastrutturaIPA.pdf);
- Indice delle Pubbliche Amministrazioni: dettaglio delle funzioni applicative (IPA - Documentazione Phase Out - Dettaglio funzioni applicative.pdf);
- Indice delle Pubbliche Amministrazioni - Metadati degli Open Data (Metadati_Open_Data.pdf);
- Schema per l'interoperabilità dell'Indice delle pubbliche amministrazioni (SPCoop-Schema_Interop_IndicePA.pdf);
- Descrizione Base Dati MySQL – Indice delle Pubbliche Amministrazioni (IPA-Descrizione data base Mysql.pdf);
- IPA - Manuale Operativo Caricamento LDAP (IPA_Manuale_operativo_-CaricamentoLDAP.pdf);
- IPA - Indice delle Pubbliche Amministrazioni - Guida all'Area Pubblica (Guida_IndicePA_Area_Pubblica.pdf);
- IPA - Indice delle Pubbliche Amministrazioni - Guida all'Area Riservata (Guida_IndicePA_Area_Riservata.pdf);
- IPA - Descrizione dei processi di accreditamento e gestione referenti (Guida_Rapida_IPA.pdf);
- Manuale operativo Service Desk IPA (Manuale_Operativo_Service_Desk_IPA.pdf).

La documentazione fa riferimento allo stato attuale del servizio. Ogni eventuale evoluzione sarà documentata all'atto della presa in carico.

[R.153] Il Fornitore deve garantire il mantenimento costante nel tempo della coerenza, della consistenza e della qualità di tutte le informazioni presenti nella base informativa del servizio, eseguendo tutti gli interventi necessari sui contenuti della stessa base informativa; tali interventi devono essere realizzati secondo quanto previsto nell'appendice "SLA e Penali" e comunque nell'ottica di minimizzare l'impatto sul servizio delle eventuali criticità.

[R.154] Il Fornitore deve garantire il costante governo di tutti i processi previsti dal servizio che assicurano, dal punto di vista tecnico/funzionale, il corretto esercizio del servizio stesso. Conseguentemente, il Fornitore deve garantire che tutti gli interventi che si dovessero rendere necessari dovranno svolgersi nell'ottica di minimizzare l'impatto delle eventuali criticità emerse sulla disponibilità e sul corretto funzionamento del servizio.

- [R.155] Il Fornitore deve progettare, concordandole con AgID, delle attività di stress-test da realizzare con cadenza quadrimestrale allo scopo di rilevare e misurare le prestazioni del sistema sotto particolari condizioni di carico. Tali attività devono essere svolte in modo da minimizzare l'impatto sul servizio in esercizio.
- [R.156] Il Fornitore deve garantire la disponibilità di un ambiente di produzione dedicato all'esercizio del servizio e di un ulteriore ambiente dedicato al collaudo/pre-esercizio e validazione di eventuali modifiche necessarie al corretto funzionamento del sistema.
- [R.157] Al fine di poter verificare il corretto funzionamento del sistema, gli utenti indicati da AgID devono poter accedere, tramite autenticazione ed in modalità sicura, all'ambiente dedicato al collaudo/pre-esercizio.
- [R.158] Il Fornitore deve garantire la corretta e tempestiva gestione delle piattaforme hw/sw, dei servizi di base e di *middleware*, necessarie al corretto funzionamento dell'IPA in tutti gli ambienti operativi disponibili.
- [R.159] Il Fornitore, nell'ambito della gestione del servizio, deve garantire una adeguata gestione delle versioni del software e mantenere allineata:
- La documentazione
 - La lista dei malfunzionamenti rilevati con l'indicazione delle relative risoluzioni.
- [R.160] Su richiesta dell'Amministrazione, il Fornitore deve garantire i **servizi di sviluppo** necessari alla manutenzione correttiva, adeguativa ed evolutiva del Servizio Indice della Pubblica Amministrazione secondo quanto previsto nel §4.5 e nel requisito [R.161]; le attività previste potranno essere volte:
- (*Manutenzione correttiva*) alla correzione di eventuali malfunzionamenti dell'applicazione
 - (*Manutenzione adeguativa*) all'adeguamento delle funzionalità del sistema resi necessari ad esempio a seguito di modifiche normative, evoluzione delle tecnologie e dei prodotti correlati
 - (*Manutenzione evolutiva*) all'aggiunta di nuove funzionalità attualmente non previste.
- [R.161] Le attività di sviluppo adeguativa ed evolutiva di cui al paragrafo 4.5 dovranno essere svolte con l'impiego delle figure professionali di cui al [R.163] e nei limiti indicati alla seguente tabella:

FIGURA PROFESSIONALE	TARIFFA MASSIMA	GG/U STIMATI
Capo Progetto	500 €	550
Analista di Business	450 €	1100
Analista Programmatore	350 €	1100
Programmatore	250 €	2200
Totale	1.705.000 €	

[R.162] L'importo totale di € 1.705.000,00 (IVA esclusa) rappresenta il limite massimo spendibile nei 60 mesi di durata contrattuale; di conseguenza, a tariffe unitarie più basse offerte potrebbe corrispondere una maggiore richiesta di attività da parte dell'Agenzia per l'Italia Digitale.

[R.163] Le figure professionali da impiegare nelle attività di sviluppo adeguata ed evolutiva dovranno corrispondere ai seguenti profili professionali minimi:

Figura professionale	Capo Progetto
Titolo di studio	Laurea o cultura equivalente (la cultura equivalente per i non laureati corrisponde a 4 anni di esperienza lavorativa aggiuntiva)
Esperienze lavorative	<ul style="list-style-type: none"> • Esperienza complessiva non inferiore a 15 anni di cui almeno 10 nella specifica funzione su progetti complessi • Significative esperienze di direzione di progetti complessi, anche in tecnologia web, in contesti multidisciplinari, multiservizi e multifornitore; • Stima di tempi e risorse necessari per realizzazione di progetto • Analisi e progettazione di sistemi informativi, package, procedure complesse • Conoscenze ed uso di tecniche e prodotti SW per

	<p>project management e risk management</p> <ul style="list-style-type: none"> • Responsabilità su gruppi di progetto
Conoscenze	<ul style="list-style-type: none"> • Metodologie di sviluppo • Metodologie di valutazione delle dimensioni di un progetto • Conoscenza della Pubblica Amministrazione • Conoscenza di tecniche e metodi di pianificazione strategica, analisi dei rischi, project management e controllo di gestione; • Conoscenza di tecniche e metodi di quality management, norme ISO, modalità di certificazione, sistemi qualità, pratica di verifiche ispettive • Conoscenza approfondita di metodi e sistemi per lo sviluppo dei sistemi informatici; • Capacità di negoziazione e di valutazione, conoscenza di contrattualistica relativa all'I.C.T., di elementi di economia e di organizzazione aziendale; • Realizzazione di business plan, studi di fattibilità, analisi costi benefici. • Conoscenza del mercato e trend evolutivi dell'I.C.T.

Figura professionale	Analista Programmatore
Titolo di studio	Laurea o cultura equivalente (la cultura equivalente per i non laureati corrisponde a 4 anni di esperienza lavorativa addizionale)
Esperienze lavorative	<ul style="list-style-type: none"> • Esperienza complessiva non inferiore a 10 anni di cui almeno 5 nella specifica funzione • Progettazione di sistemi software di grandi dimensioni basati su tecnologie "object oriented" • Significative esperienze di direzione di progetti software complessi

	<ul style="list-style-type: none"> • Capacità di sviluppare adeguate metodologie per i test; • Capacità di realizzare documentazione tecnica (questa implica una buona capacità di sintesi e, al contempo, di chiarezza) • Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione di applicazioni, anche accessibili in modalità web • Stima di tempi e risorse necessari per la realizzazione di progetti • Esperienza nell'utilizzo di metodologie di project management
Conoscenze	<ul style="list-style-type: none"> • Metodologie di disegno di prodotti software • DBMS relazionali, SQL • Strumenti di modellazione dati • Tecniche di programmazione Object Oriented • Strumenti per il cleaning e la qualità dei dati • Sistemi LDAP con particolare riferimento alla piattaforma OpenLDAP • Strumenti di ETL • Web designer (grafico) • Ottima conoscenza di tecniche di configuration management del software • Conoscenza delle problematiche di sicurezza on line

Figura professionale	Analista di Business
Titolo di studio	Laurea o cultura equivalente (la cultura equivalente per i non laureati corrisponde a 4 anni di esperienza lavorativa addizionale)
Esperienze lavorative	<ul style="list-style-type: none"> • Esperienza complessiva non inferiore a 10 anni di cui almeno 5 nella specifica funzione • Analisi dei requisiti utente • Analisi funzionale di applicazioni, anche di tipo web • Coordinamento di gruppi di lavoro nell'ambito di progetti di realizzazione di applicazioni, anche accessibili in modalità web

	<ul style="list-style-type: none"> • Stima di tempi e risorse necessari per la realizzazione di progetti • Esperienza nell'utilizzo di metodologie di project management • Capacità di problem solving
Conoscenze	<ul style="list-style-type: none"> • Conoscenza delle caratteristiche dei principali ambienti di sviluppo di applicazioni anche di tipo web • Redazione di specifiche di progetto in ambiente web services • Conoscenza del mercato e delle tendenze evolutive dell'I.C.T. per quanto attiene lo sviluppo e l'integrazione in modalità web di applicazioni

Figura professionale	Programmatore
Titolo di studio	Diploma di perito informatico o cultura superiore in ambito tecnico-scientifico
Esperienze lavorative	<ul style="list-style-type: none"> • Anzianità minima di 3 anni come programmatore • Sviluppo di analisi tecnica di bassa complessità • Progettazione ed Esecuzione di test • Preparazione di documentazione di programmi • Partecipazione alla stesura di specifiche tecniche • Partecipazione a gruppi di progetto di medie dimensioni • Programmazione in ambiente client-server, Web e SOA • Metodologie di analisi, disegno di prodotti SW • Installazione e personalizzazione di sistemi anche complessi • Progettazione ed integrazione di sistemi • Strumenti per la codifica dei programmi • Tecniche di programmazione strutturata
Conoscenze	<ul style="list-style-type: none"> • Ha una completa autonomia nello sviluppo, nella preparazione ed esecuzione di casi di test di unità, nella preparazione di documentazione di programmi, nella stesura di specifiche tecniche. • Strumenti per la codifica dei programmi • DBMS relazionali, SQL • Tecniche di programmazione

- [R.164] Il Fornitore deve garantire un servizio **Service Desk IPA** di supporto operativo all'utente e ad AgID, che gestisca tutte le richieste, sia di servizio sia di tipo informativo, provenienti dai soggetti titolati ad essere accreditati presso l'IPA, dai cittadini e dalle imprese. Il Service Desk IPA deve rappresentare l'interfaccia unica per i seguenti processi:
- Accreditamento;
 - Gestione referenti;
 - Cancellazione di un ente;
 - Segnalazioni di criticità e anomalie.
- [R.165] Il Fornitore deve, per ogni processo di cui al requisito [R.164], espletare tutte le verifiche necessarie a garantire la correttezza, completezza e adeguatezza normativa e amministrativa delle azioni realizzate.
- [R.166] Il Fornitore deve rendere disponibile un punto unico di contatto per il servizio di cui al requisito [R.164], raggiungibile attraverso:
- Un numero unico telefonico. Dovrà trattarsi di un "Numero Verde", le chiamate dovranno cioè essere gratuite (c.d. addebito al chiamato) nel caso siano originate da rete fissa nazionale;
 - Posta elettronica;
 - PEC.
- [R.167] Il Service Desk deve garantire:
- La corretta conservazione ed il reperimento di tutte le richieste utente legate ai processi di cui al requisito [R.164] e della relativa ulteriore documentazione a corredo;
 - La gestione di una Knowledge Base contenente un elenco delle soluzioni alle problematiche note in modo da poter individuare direttamente la soluzione senza procedere ad escalation verso i livelli superiori.
- [R.168] Il Fornitore deve garantire che almeno una parte del personale coinvolto abbia una provata competenza in diritto, CAD (Codice dell'Amministrazione Digitale) e normativa della PA. Il Fornitore deve garantire la disponibilità di un competence center costituito da personale che abbia almeno una quadriennale esperienza in diritto amministrativo, con competenze specifiche

su organizzazione della PA e CAD. AgID avrà la facoltà di approvare le risorse costituenti il suddetto competence center.

[R.169] Il Service Desk IPA dovrà essere disponibile tutti i giorni lavorativi dell'anno, dal lunedì al venerdì dalle ore 08:00 alle ore 20:00, il sabato dalle ore 08:00 alle ore 14:00.

2.4 Servizio Indice dei Gestori PEC (IGPEC)

[R.170] Il servizio Indice dei Gestori di Posta Elettronica Certificata (IGPEC) comprende:

- La presa in carico del servizio garantendo senza soluzione di continuità la disponibilità di tutte le funzionalità fino al termine della fase di migrazione;
- La progettazione, realizzazione e messa in esercizio del nuovo ambiente di produzione dedicato del servizio e dell'ambiente dedicato al collaudo/pre-esercizio secondo l'architettura prevista al requisito [R.171];
- La progettazione e realizzazione della fase di migrazione dell'attuale sistema nel rispetto del requisito [R.171];
- La gestione dei processi di inserimento di nuovi Gestori PEC ovvero di eventuale aggiornamento/rimozione di Gestori PEC già presenti in IGPEC;
- La gestione ed il monitoraggio del servizio, inclusa la manutenzione e la gestione sistemistica dell'ambiente di produzione;
- La manutenzione correttiva, adeguativa ed evolutiva di tutte le componenti del servizio.

[R.171] Il Fornitore deve acquisire tutte le informazioni necessarie per l'erogazione del servizio dal documento in appendice 6 'Infrastruttura IGPEC - Documentazione tecnica' (InfrastrutturaIGPEC.pdf), in cui sono specificate le finalità, le funzionalità e l'architettura dell'IGPEC.

- [R.172] Il Fornitore deve implementare un sistema di autenticazione per la verifica degli accessi all'IGPEC, come descritta nel documento di cui al requisito [R.171].
- [R.173] Il Fornitore deve garantire la tempestiva introduzione, ovvero la cancellazione, di un Gestore PEC all'interno del processo descritto nel precedente requisito, secondo le indicazioni che riceverà da Agenzia per l'Italia Digitale.
- [R.174] Il Fornitore deve garantire l'acquisizione e il relativo controllo dei contenuti che ogni Gestore PEC rende disponibili. Tale processo opera secondo i tempi indicati da Agenzia per l'Italia Digitale.
- [R.175] Il Fornitore deve garantire il mantenimento costante nel tempo della coerenza, della consistenza e della qualità di tutte le informazioni presenti nella base informativa del servizio, eseguendo tutti gli interventi necessari sui contenuti della stessa base informativa; tali interventi devono essere realizzati tempestivamente al fine di minimizzare l'impatto sul servizio di eventuali criticità.
- [R.176] Il Fornitore deve garantire il costante governo di tutti i processi previsti dal servizio che assicurano, dal punto di vista tecnico/funzionale, il corretto esercizio del servizio stesso. Conseguentemente, il Fornitore deve garantire che tutti gli interventi che si dovessero rendere necessari dovranno svolgersi nell'ottica di minimizzare l'impatto delle eventuali criticità emerse sulla disponibilità e sul corretto funzionamento del servizio.
- [R.177] Il Fornitore deve garantire la disponibilità di un ambiente di produzione dedicato all'esercizio del servizio e di un ulteriore ambiente dedicato al collaudo/pre-esercizio e validazione di eventuali modifiche necessarie al corretto funzionamento del sistema.
- [R.178] Al fine di poter verificare il corretto funzionamento del sistema, gli utenti indicati da AgID devono poter accedere, tramite autenticazione ed in modalità sicura, all'ambiente dedicato al collaudo/pre-esercizio.
- [R.179] Il Fornitore deve garantire la corretta e tempestiva gestione delle piattaforme hw/sw, dei servizi di base e di middleware, necessarie al corretto funzionamento dell'IGPEC in tutti gli ambienti operativi disponibili.
- [R.180] Il Fornitore, nell'ambito della gestione del servizio, deve garantire una adeguata gestione delle versioni del software e mantenere allineata:
- La documentazione
 - La lista dei malfunzionamenti rilevati con l'indicazione delle relative risoluzioni.

[R.181] Su richiesta dell'Amministrazione, il Fornitore deve garantire i **servizi di sviluppo** necessari alla manutenzione correttiva, adeguativa ed evolutiva del Servizio Indice dei Gestori PEC secondo quanto previsto nel §4.5; le attività previste potranno essere volte:

- *(Manutenzione correttiva)* alla correzione di eventuali malfunzionamenti dell'applicazione
- *(Manutenzione adeguativa)* all'adeguamento delle funzionalità del sistema resi necessari ad esempio a seguito di modifiche normative, evoluzione delle tecnologie e dei prodotti correlati
- *(Manutenzione evolutiva)* all'aggiunta di nuove funzionalità attualmente non previste.

[R.182] Le attività di manutenzione adeguativa ed evolutiva di cui al paragrafo 4.5 dovranno essere svolte con l'impiego delle figure professionali di cui al [R.184] e nei limiti indicati alla seguente tabella:

FIGURA PROFESSIONALE	TARIFFA MASSIMA	GG/U STIMATI
Analista Programmatore	350 €	320
Totale	112.000 €	

[R.183] L'importo totale di € 112.000,00 (IVA esclusa) rappresenta il limite massimo spendibile nei 60 mesi di durata contrattuale; di conseguenza, a tariffe unitarie più basse offerte potrebbe corrispondere una maggiore richiesta di attività da parte dell'Agenzia per l'Italia Digitale.

[R.184] Le figure professionali da impiegare nelle attività di sviluppo adeguativa ed evolutiva dovranno corrispondere al profilo Analista Programmatore definito al requisito [R.163].

3 Servizi di Governance (SGOV)

[R.185] I servizi di Governance di SPC2 sono erogati esclusivamente verso

- i Fornitori Qualificati SPC2 per i servizi di Connettività;
- i Fornitori dei “Servizi Applicativi”, individuati mediante gara a procedura ristretta, suddivisa in quattro lotti, per l’affidamento dei servizi di Cloud Computing, di Sicurezza, di Realizzazione di Portali e Servizi on-line e di Cooperazione Applicativa per le Pubbliche Amministrazioni” - ID 1403, pubblicata il 24/12/2013;
- i soggetti sussidiari (nelle modalità previste dal DPCM 1 aprile 2008 recante le “Regole Tecniche per i servizi di connettività e sicurezza SPC previste dall’articolo 71, comma 1-bis del decreto legislativo 7 marzo 2005, n.82, recante il <<Codice dell’amministrazione digitale>>”);
- il CERT-PA, struttura che opera presso l’AgID ed è preposta al trattamento degli incidenti di sicurezza informatica all’interno del dominio costituito dalle Pubbliche Amministrazioni nazionali, secondo quanto previsto dal DPCM 24/1/2013;
- AgID, Consip e le pubbliche amministrazioni in genere, nelle modalità descritte nei paragrafi successivi.

[R.186] I Servizi di Governance comprendono:

- a **Servizio di Gestione Automatizzata dei Contratti (SGAC):** gestisce i dati economici, di consistenza e tecnici delle singole istanze di servizio contrattualizzate dalle Amministrazioni; attraverso interfacce web permette la corretta compilazione dei Piani dei Fabbisogni (PIF) (da parte delle Amministrazioni) e dei Progetti dei Fabbisogni (da parte dei Fornitori Qualificati SPC²), nel rispetto dei vincoli espressi nei Contratti Quadro;
- b **Servizio di Gestione dei Dati di Qualità e Sicurezza (SGQS):** permette il monitoraggio della qualità e della sicurezza dei servizi erogati all’interno di SPC², attraverso la raccolta e l’analisi dei Key Performance Indicator (KPI) dei servizi erogati alle Amministrazioni dai Fornitori Qualificati SPC²;
- c **Servizio di Gestione delle Escalation (SGES):** consente la gestione dei malfunzionamenti e degli incidenti di sicurezza che richiedono interventi di *escalation*, ovvero che impattano due o più Fornitori Qualificati SPC²;
- d **Servizio di Gestione dell’Accesso Web (SGAW):** punto di accesso a tutti i servizi d’interoperabilità ed ai servizi di governance di cui ai punti a), b) e c), contiene elementi informativi personalizzati in funzione dell’utenza che vi accede, come specificato in dettaglio nei paragrafi successivi.

- [R.187] I servizi di cui al requisito [R.186] devono essere erogati attraverso un'unica infrastruttura informatica – denominata in seguito Infrastruttura informatica per l'erogazione dei Servizi di Governance – integrata e accessibile tramite il web. Il Fornitore dovrà sviluppare e fornire ad AgID, nonché gestire presso il Data Center di cui al requisito [R.4], tutte le componenti hardware e software che compongono tale infrastruttura.
- [R.188] Il Fornitore deve rendere disponibile un servizio DNS con il quale esporre/gestire le zone e i relativi host associati ai servizi del presente capitolo. A seconda delle caratteristiche del singolo servizio le zone devono essere pubblicate o sulla Rete Internet/Infranet o sulla Rete Infranet.
- [R.189] I servizi di cui al requisito [R.186] devono essere integrati secondo la logica riportata in Figura 13.
- [R.190] A titolo esemplificativo ma non esaustivo la suddetta integrazione deve consentire
- Il recupero dei dati di qualità e sicurezza di un determinato contratto esecutivo;
 - L'associazione tra un ticket di escalation e i contratti esecutivi – e quindi le amministrazioni – coinvolti;
 - La realizzazione di cruscotti personalizzati evoluti in cui sia possibile correlare informazioni contrattuali, gestionali ed operative.



Figura 13

- [R.191] L'Infrastruttura informatica per l'erogazione dei Servizi di Governance deve prevedere un servizio di repository centrale che implementi le funzioni di

Raccolta, Gestione, Conservazione ed Archiviazione dei dati e che sia realizzato tramite le seguenti componenti:

- *Interfaccia di raccolta dati* che riceve/preleva i dati tramite server web di presentazione;
- *Repository* modellato in una struttura composta da un livello di Data Warehouse Centrale (DWC) e dei Data Mart (DM) specifici;
- *ETL (Extract, Transform and Load) Manager* che si occupa della riconciliazione, transcodifica, standardizzazione, aggregazione, controllo della qualità e completezza dei dati.

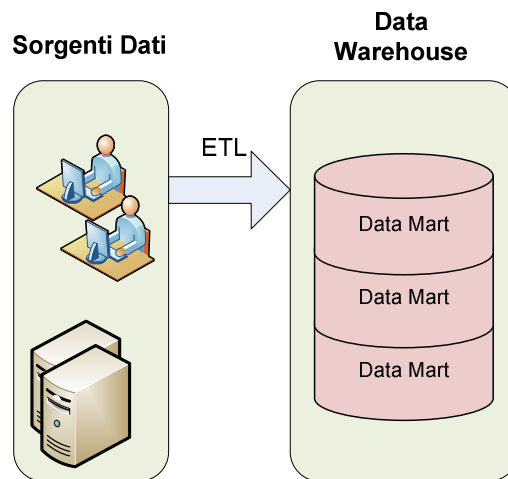


Figura 14

[R.192] L'Infrastruttura informatica per l'erogazione dei Servizi di Governance deve essere progettata per garantire confidenzialità, integrità e disponibilità dei dati e, anche coerentemente con quanto definito al requisito [R.7], soddisfare almeno le seguenti specifiche:

- Servizio di controllo del flusso tramite firewall, per potere realizzare la segmentazione in zone di sicurezza e controllare i flussi ammessi tra le diverse zone; deve essere fornita una classificazione delle zone di sicurezza individuate nell'infrastruttura e, in accordo con AgID, una matrice di controllo dei flussi tra le diverse zone;
- Servizio di Network Intrusion Detection/Prevention;

- Antivirus per la protezione della posta ed il flusso di navigazione HTTP dal Sistema di Governance ad Internet;
- Servizio di monitoraggio dello stato dei sistemi che riporti lo stato di disponibilità degli stessi;
- Servizio di archiviazione e ripristino automatico dei dati.

[R.193] Il Fornitore deve realizzare un sistema di *Identity Management* che implementi almeno le seguenti funzionalità:

- Gestione dell'anagrafica degli utenti tramite un database specializzato ed ottimizzato nelle operazioni di lettura e ricerca;
- Web Access Management che, tramite opportune policies, autorizza i diversi profili di utenti ad accedere a determinati servizi web, ftp, sftp e Web Services;
- Password Management che consente di effettuare operazioni di Self service password reset;
- Profile Update che consente all'utente abilitato di aggiornare autonomamente parte dei dati relativi alla sua anagrafica.

[R.194] Il sistema di *Identity Management* deve essere implementato in accordo con i macroblocchi funzionali riportati in Figura 15.

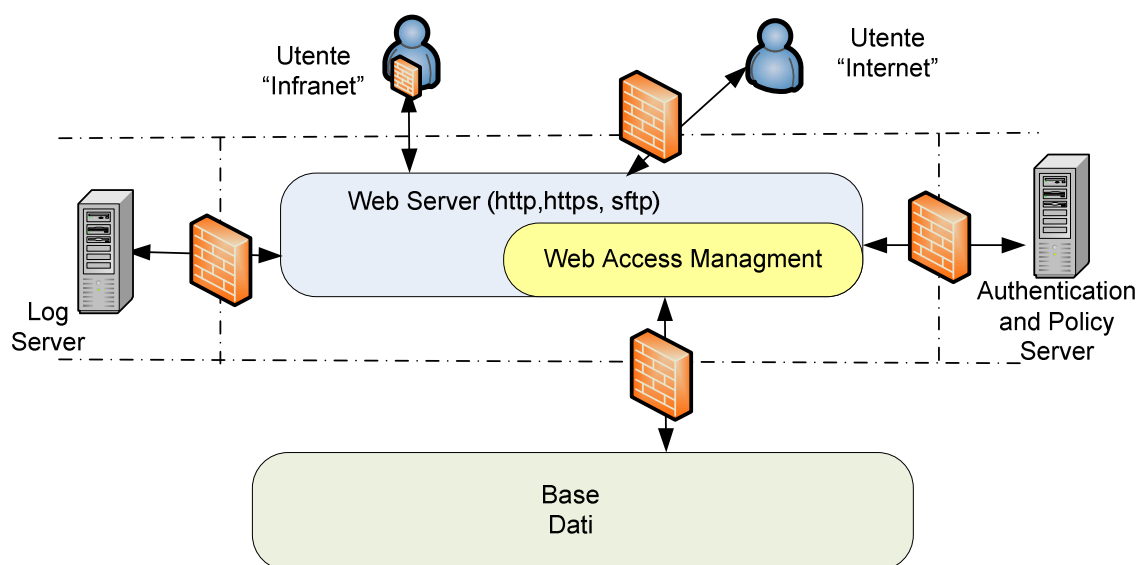


Figura 15

- [R.195] Il sistema di Identity Management deve essere configurato per soddisfare i requisiti [R.234] e [R.246].
- [R.196] Il Fornitore deve garantire l'alta affidabilità di tutte le componenti dell'infrastruttura informatica per l'erogazione dei Servizi di Governance.
- [R.197] L'infrastruttura informatica per l'erogazione dei Servizi di Governance deve essere opportunamente dimensionata per:
- Gestire circa 5.000 contratti esecutivi e 1.500.000 istanze di servizio
 - Assicurare le prestazioni definite nell'appendice "SLA e Penali" almeno per un carico di interrogazioni di 500 all'ora.
- [R.198] Il Fornitore è inoltre tenuto ad adeguare l'infrastruttura informatica per l'erogazione dei Servizi di Governance al raggiungimento del limite di cui sopra, previa valutazione degli eventuali oneri che saranno oggetto di valutazione di congruità tecnico/economica.
- [R.199] Il Fornitore è tenuto a progettare e realizzare, per ogni servizio descritto nei paragrafi successivi, uno o più Manuali Operativi in cui vengano descritte, con una logica step-by-step, tutti i processi, le regole tecniche, le azioni e le procedure da eseguire per la corretta interazione, il corretto utilizzo operativo e la corretta gestione amministrativa dell'infrastruttura informatica per l'erogazione dei Servizi di Governance.
- [R.200] Il Fornitore deve garantire la conservazione per tutta la durata contrattuale dei dati raccolti ed elaborati da tutti i Servizi di Governance; tali dati, alla scadenza del contratto, devono essere consegnati all'AgID su supporto ed in formato aperto da concordare entrambi con AgID.
- [R.201] Il Fornitore, al termine del periodo contrattuale previsto, dovrà fornire tutte le indicazioni tecniche e procedurali per la gestione ed amministrazione di tutte le componenti hardware e software dell'Infrastruttura informatica per l'erogazione dei Servizi di Governance, oggetto di fornitura ad AgID.
- [R.202] Le attività di manutenzione adeguativa ed evolutiva di cui al paragrafo 4.5 dovranno essere svolte con l'impiego delle figure professionali di cui al [R.204] e nei limiti indicati alla seguente tabella:

FIGURA PROFESSIONALE	TARIFFA MASSIMA	GG/U STIMATI
Capo Progetto	500 €	100

Analista Programmatore	350 €	300
Programmatore	250 €	1500
Totale	530.000 €	

[R.203] L'importo totale di € 530.000,00 (IVA esclusa) rappresenta il limite massimo spendibile nei 60 mesi di durata contrattuale; di conseguenza, a tariffe unitarie più basse offerte potrebbe corrispondere una maggiore richiesta di attività da parte dell'Agenzia per l'Italia Digitale.

[R.204] Le figure professionali da impiegare nelle attività di sviluppo adeguativa ed evolutiva dovranno corrispondere ai seguenti profili professionali minimi:

Capo Progetto IT	
Titolo di Studio	Laurea in discipline tecnico-scientifiche
Esperienze Lavorative	<ul style="list-style-type: none"> Anzianità lavorativa di almeno 12 anni, con almeno 4 di provata esperienza lavorativa nella specifica funzione su progetti complessi. E' particolarmente apprezzata la conoscenza del settore pubblico, preferibilmente nella Pubblica Amministrazione italiana. Almeno 2 anni di provata esperienza di analisi e progettazione di sistemi informativi, package e procedure complesse nel settore pubblico, con periodi di permanenza continuativa presso lo stesso cliente non inferiori a 6 mesi. Almeno il possesso di una tra le seguenti certificazioni: PMP, CAPM o Prince2.
Conoscenze	<ul style="list-style-type: none"> Metodologie di project management e risk management Metodologie di sviluppo SW Redazione di specifiche di progetto Controllo realizzazione procedure Stima di risorse per realizzazione di progetto Stima di tempi Analisi e progettazione di sistemi informativi, package, procedure complesse Conoscenze ed uso di tecniche e prodotti SW per project management e risk management Responsabilità su gruppi di progetto Standard ITIL

Analista Programmatore	
Titolo di Studio	Diploma di perito informatico o cultura superiore in ambito tecnico-scientifico

Esperienze Lavorative	<ul style="list-style-type: none"> • Anzianità minima di 4 anni come programmatore e di 1 anno nella funzione • Coordinamento di piccoli gruppi di lavoro • Verifica della corretta applicazione di metodi e standard • Sviluppo di analisi tecnica di media complessità • Documentazione di procedure • Programmazione strutturata, in ambiente client-server, Web e SOA • Preparazione casi di test ed esecuzione di test • Predisposizione di script per il testing automatico con i principali prodotti per il testing automatico • Partecipazione a gruppi di progetto di medie/grandi dimensioni • Tecnologie emergenti • Metodologie di analisi e disegno di prodotti SW • Installazione e personalizzazione di sistemi anche complessi • Progettazione ed integrazione di sistemi • Tecniche di programmazione strutturata • Pacchetti software relativi al progetto
Conoscenze	<ul style="list-style-type: none"> • Metodologie di disegno di prodotti software • DBMS relazionali, SQL • Strumenti di modellazione dati • Tecniche di programmazione Object Oriented • Strumenti per il cleaning e la qualità dei dati • Strumenti di ETL • Web designer (grafico) • Ottima conoscenza di tecniche di configuration management del software

Programmatore	
Titolo di Studio	Diploma di perito informatico o cultura superiore in ambito tecnico-scientifico
Esperienze Lavorative	<ul style="list-style-type: none"> • Anzianità minima di 3 anni come programmatore • Sviluppo di analisi tecnica di bassa complessità • Progettazione ed Esecuzione di test • Preparazione di documentazione di programmi • Partecipazione alla stesura di specifiche tecniche • Partecipazione a gruppi di progetto di medie dimensioni • Programmazione in ambiente client-server, Web e SOA • Metodologie di analisi, disegno di prodotti SW • Installazione e personalizzazione di sistemi anche complessi • Progettazione ed integrazione di sistemi • Strumenti per la codifica dei programmi • Tecniche di programmazione strutturata
Conoscenze	<ul style="list-style-type: none"> • Ha una completa autonomia nello sviluppo, nella preparazione ed esecuzione di casi di test di unità, nella preparazione di documentazione di programmi, nella stesura di specifiche tecniche. • Strumenti per la codifica dei programmi • DBMS relazionali, SQL • Tecniche di programmazione

3.1 Servizio di Gestione Automatizzata dei Contratti (SGAC)

[R.205] Il Fornitore deve progettare, realizzare, fornire, gestire e monitorare l'infrastruttura informatica che realizza il Servizio di Gestione Automatizzata dei Contratti in modo da garantire gli specifici requisiti indicati nel presente Capitolato Tecnico.

[R.206] L'infrastruttura informatica di cui al requisito [R.205] deve essere costituita almeno dalle seguenti componenti logiche, come evidenziato in Figura 16:

- **Anagrafe Unica dei Contratti (AUC):** base dei dati contrattuali SPC²;
- **Create, Read, Update e Delete (CRUD):** interfaccia per le operazioni *CRUD* sulla AUC;
- **Logica di Controllo del Workflow Contrattuale (LCWC):** sistema automatico per la verifica della correttezza dei dati su AUC, con eventuale allarme sul sistema CRUD.

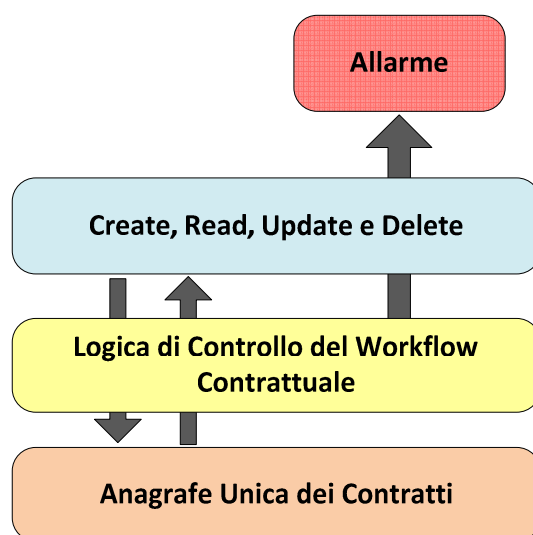


Figura 16

[R.207] Il Fornitore deve costituire la piattaforma informatica Anagrafe Unica dei Contratti SPC2 (AUC), contenente tutti i dati normativi, contrattuali e tecnici di ciascun Contratto Quadro e dei relativi Contratti Esecutivi (inclusi eventuali allegati) stipulati dalle Amministrazioni.

[R.208] Il Fornitore deve predisporre interfacce per la consultazione da parte di AgID della piattaforma AUC almeno in modalità Structured Query Language (SQL), in modalità sicura. Il Concorrente può evidenziare la disponibilità di ulteriori modalità di interfacce.

[R.209] Il Fornitore deve rendere disponibile il sistema CRUD (Create, Read, Update e Delete), per la corretta ed univoca modellazione dei Piani dei Fabbisogni (da parte delle Amministrazioni) e dei Progetti dei Fabbisogni (da parte dei Fornitori Qualificati SPC²) attraverso:

- Un'interfaccia *web form* alla piattaforma AUC messa a disposizione attraverso il Servizio di Gestione dell'Accesso Web di IC-SPC (cfr. § 3.4);
- Un'interfaccia *Web Service*.

Il Concorrente può evidenziare la disponibilità di ulteriori modalità di interfacce.

[R.210] Il sistema di Logica di Controllo del Workflow Contrattuale (LCWC) deve garantire il corretto workflow delle procedure contrattuali attraverso un controllo di consistenza sui dati dell'AUC; in particolare deve essere in grado di:

- a) Rilevare eventuali inconsistenze sui dati contrattuali inseriti nella AUC;
- b) Avvisare tramite il sistema CRUD il soggetto impattato (AgID, Amministrazione o Fornitore Qualificato SPC²).

[R.211] L'infrastruttura della AUC deve prevedere almeno le seguenti strutture dati:

- Contratti Quadro (e, eventuali, successivi Atti Aggiuntivi);
- Fornitori SPC², con i relativi referenti;
- Catalogo dei servizi per ciascun Contratto Quadro attivo (includente, per ogni servizio, le caratteristiche tecniche, i relativi parametri dimensionali ed il prezzo);
- Pubbliche Amministrazioni contraenti;
- Contratti Esecutivi, relativi Piani dei Fabbisogni (con i relativi servizi richiesti) e Progetti dei Fabbisogni con annessi Piani di Attuazione (con relativi servizi contrattualizzati);

A titolo esemplificativo e non esaustivo nella figura successiva si riporta lo schema concettuale dell'Anagrafica Unica dei Contratti.

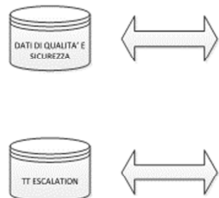


Figura 17

[R.212] Il Servizio di Gestione Automatizzata dei Contratti deve consentire l'interazione, attraverso interfaccia web, tra la P.A. che ha aderito o intende aderire al SPC² e il Fornitore SPC², supportando tutte quelle funzionalità necessarie alla realizzazione e sottoscrizione di un contratto esecutivo. In particolare deve poter consentire:

- Il caricamento delle informazioni relative alla anagrafica del Fornitore SPC² e a quella delle Pubbliche Amministrazioni con cui viene sottoscritto un contratto esecutivo;
- La compilazione di webform relative al workflow di gestione "Piano dei Fabbisogni";
- La compilazione di webform relative al workflow di gestione dei "Progetto dei Fabbisogni"; la gestione on line del Progetto dei Fabbisogni e dell'eventuale processo di migrazione dei servizi;
- La sottoscrizione del contratto esecutivo tramite firma digitale o, in alternativa, l'upload del contratto sottoscritto dalle parti;
- L'agevole associazione tra contratto quadro, contratto esecutivo, piano dei fabbisogni, progetto dei fabbisogni e suoi allegati contenuti nel Repository documentale (ad esempio Piano di Attuazione).

La figura seguente schematizza la sequenza logica che regola i legami tra le informazioni contenute nell'anagrafica delle Amministrazioni e dei fornitori, in contratti esecutivi, i piani ed i progetti dei fabbisogni.

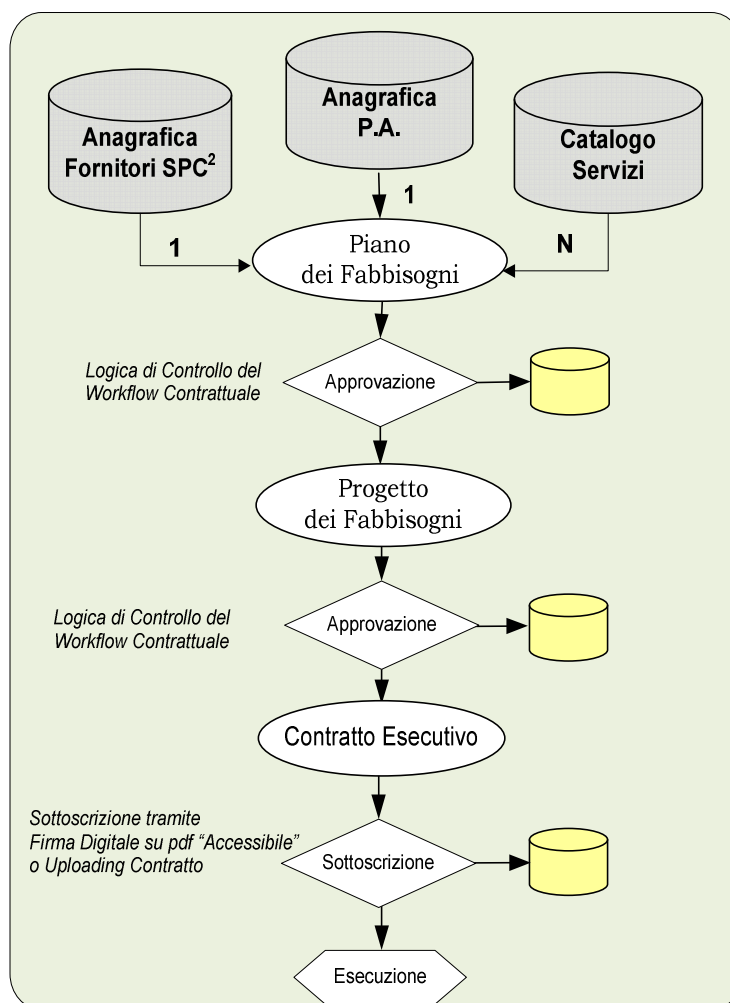


Figura 18

- [R.213] Il Fornitore deve garantire la manutenzione adeguativa (secondo quanto previsto nel §4.5, requisiti [R.202], [R.203] e [R.204]), su richiesta di AgID, di tutte le piattaforme dell'infrastruttura per la realizzazione del Servizio di Gestione Automatizzata dei Contratti, anche in corso d'opera, a fronte dell'inserimento di nuovi servizi in Contratti Quadro (Atti Aggiuntivi) in essere o della stipula di un nuovo Contratto Quadro.
- [R.214] Nel caso in cui l'inserimento di Atti Aggiuntivi o di nuovi Contratti Quadro non richieda modifiche alla struttura delle tabelle del data base, i relativi interventi di manutenzione sono ricompresi nel canone del servizio e non saranno soggetti ad oneri aggiuntivi.

3.2 Servizio di Gestione dei Dati di Qualità e Sicurezza (SGQS)

[R.215] Il Fornitore deve progettare, realizzare, fornire, gestire e monitorare l'infrastruttura informatica che realizza il Servizio di Gestione dei Dati di Qualità e Sicurezza in modo da garantire gli specifici requisiti indicati nel presente Capitolato Tecnico.

[R.216] L'infrastruttura informatica di cui al requisito [R.215] deve essere costituita almeno dalle seguenti piattaforme:

- **Dati di Qualità e Sicurezza (DQS):** base dei dati di qualità e sicurezza forniti dai Fornitori SPC² e dalle Infrastrutture Condivise -SPC;
- **Caricamento Massivo dei KPI (CMK):** strumento per il caricamento massivo dei *Key Performance Indicator* (KPI) sul DQS;
- **Logica di Controllo della Corrispondenza dei KPI (LCCK):** sistema automatico per la verifica del corretto caricamento dei dati sul DQS e della loro corrispondenza con i dati AUC.

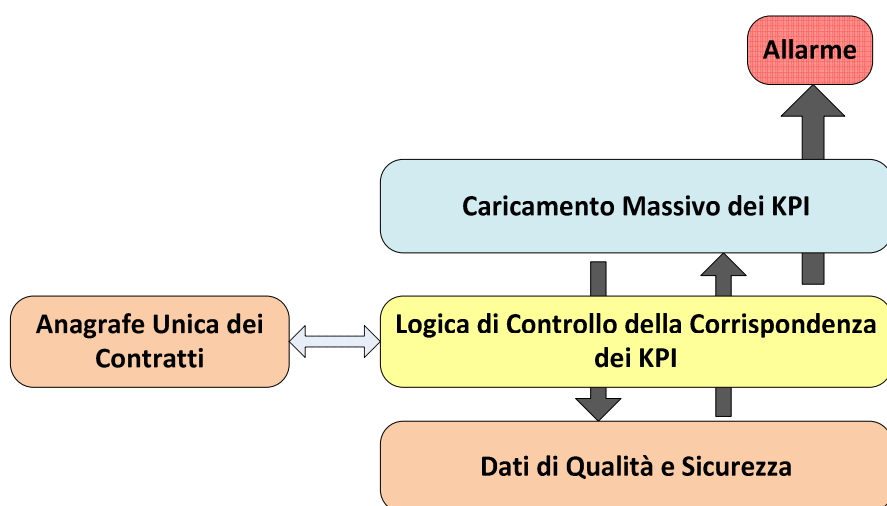


Figura 19

[R.217] Il Fornitore deve costituire la piattaforma informatica Dati di Qualità e Sicurezza (DQS), contenente i dati di qualità e sicurezza relativi ai Key Performance Indicator (KPI) di tutti i servizi erogati dai Fornitori SPC², compresi i KPI delle IC-SPC e i dati economici relativi ai KPI dei Fornitori SPC².

[R.218] Il Fornitore deve predisporre interfacce per la consultazione da parte di AgID della piattaforma DQS almeno in modalità Structured Query Language (SQL), in modalità sicura. Il Concorrente può evidenziare la disponibilità di ulteriori modalità di interfacce.

[R.219] Il Fornitore deve rendere disponibile il sistema “Caricamento Massivo dei KPI” per il caricamento massivo (con frequenza mensile) dei KPI sul DQS da parte dei Fornitori SPC², attraverso:

- Una interfaccia Secure File Transfer Protocol (SFTP);
- Una interfaccia Web Service.

Il Concorrente può evidenziare la disponibilità di ulteriori modalità di interfacce.

[R.220] Il sistema di Logica di Controllo della Corrispondenza dei KPI (LCCK) deve garantire il corretto caricamento e la corrispondenza dei KPI di cui al requisito [R.217] con i dati contenuti nel sistema “Anagrafe Unica dei Contratti” (AUC).

[R.221] Il sistema di Logica di Controllo della Corrispondenza dei KPI (LCCK) deve:

- a) Rilevare eventuali errori di invio/ricezione nel caricamento massivo dei dati DQS;
- b) Rilevare eventuali non corrispondenze tra i dati DQS inviati e i dati del sistema AUC;
- c) Avvisare tramite CMK il soggetto impattato (AgID, Fornitore SPC²) al verificarsi degli eventi di cui ai punti a) e b), al fine di permettere a tale soggetto di gestire, effettuando le opportune azioni correttive, gli allarmi ricevuti su apposita dashboard dalla Logica di Controllo della Corrispondenza dei KPI (LCCK).

[R.222] Il Fornitore deve garantire che la piattaforma DQS sia in grado di gestire almeno le seguenti strutture dati:

- KPI relativi ai singoli servizi SPC²;
- KPI economici relativi al Fornitore SPC².

Le strutture dati devono rispettare le specifiche ed il formato definiti all'interno del documento “**Regole di Interconnessione per l'adesione ai servizi di Governance**” (cfr. [R.333]). A titolo di esempio si riporta il dettaglio di alcune di queste strutture:

- KPI relativi ai singoli servizi SPC²: data di inizio e data fine erogazione, quantità di componenti di servizio attive,

disponibilità del servizio, Trouble Ticket associati e chiusi (con severità, causa disservizio e tempo di ripristino, etc.);

- KPI economici relativi al Fornitore SPC²: valore complessivo del contrattualizzato, valore complessivo delle penali su ciascun servizio, valore del fatturato annuale di ogni singolo contratto esecutivo, etc.

[R.223] Il Fornitore deve garantire l'adeguamento, su richiesta di AgID, di tutte le piattaforme dell'infrastruttura per la realizzazione del Servizio di Gestione dei Dati di Qualità e Sicurezza, anche in corso d'opera, previa valutazione degli eventuali oneri che saranno oggetto di valutazione di congruità tecnico/economica.

3.3 Servizio di Gestione delle Escalation (SGES)

[R.224] Il Fornitore deve progettare, realizzare, fornire, gestire e monitorare l'infrastruttura informatica che realizza il Servizio di Gestione delle Escalation in modo da garantire gli specifici requisiti indicati nel presente Capitolato Tecnico.

[R.225] L'infrastruttura informatica di cui al requisito [R.224] deve essere integrata all'interno del Servizio di Gestione dell'Accesso Web (cfr. §3.4) attraverso una web form e deve garantire la registrazione e il tracciamento di tutti gli eventi di escalation relativi ai servizi di trasporto dati, di sicurezza e di comunicazione evoluta SPC².

[R.226] La piattaforma messa a disposizione dal Fornitore deve permettere la segnalazione, da parte delle Unità Locali di Sicurezza SPC (ULS¹) o da parte di un soggetto attestato alle IC-SPC, di eventuali problematiche di connettività o di sicurezza che coinvolgono altri soggetti SPC² attestati alle IC-SPC.

[R.227] Dove possibile, la piattaforma deve agevolare attraverso l'accesso al sistema di "Anagrafe Unica dei Contratti", la corretta individuazione dei referenti per la sicurezza dei Fornitori SPC² coinvolti nella segnalazione.

[R.228] La Piattaforma deve garantire la segnalazione ai soggetti interessati dall'evento di escalation, almeno tramite e-mail. Il Concorrente può evidenziare la disponibilità di ulteriori modalità di segnalazione (es. sms, sistemi di messaggistica istantanea, ecc.)

¹ definite dal DPCM 1 aprile 2008, art. 21, comma 6

- [R.229] La Piattaforma, deve garantire ad AgID, per tutta la durata contrattuale, la consultazione in tempo reale di tutti gli eventi tracciati.

3.4 Servizio di Gestione dell'Accesso Web (SGAW)

- [R.230] Il Fornitore deve progettare, realizzare, fornire, gestire e monitorare l'infrastruttura informatica che realizza il Servizio di Gestione dell'Accesso Web (SGAW) in modo da garantire gli specifici requisiti indicati nel presente Capitolato Tecnico.

- [R.231] L'infrastruttura informatica di cui al requisito [R.230] deve essere costituita da una piattaforma di Content Management System (CMS) in grado di gestire il ciclo di vita dei contenuti, attraverso il seguente workflow:

- Redazione;
- Verifica/modifica e approvazione;
- Pubblicazione;
- Manutenzione e dismissione.

- [R.232] La piattaforma CMS deve prevedere le seguenti funzionalità generali:

- SEO - Search Engine Optimization: permette l'ottimizzazione del sito per la visibilità sui più comuni motori di ricerca;
- Versioning dei contenuti: permette la gestione delle revisioni dei contenuti del sito web relative agli ultimi 30 giorni;
- Storizzazione dei contenuti: permette il salvataggio e il ripristino dei contenuti del sito web relativi agli ultimi 30 giorni;
- Accessibilità: in conformità a quanto stabilito dalla Legge n.4 del 9 gennaio 2004, dal D.M. 8 luglio 2005 pubblicato nella G.U. del 8 agosto 2005 nonché dal decreto legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012, n. 221 in tema di accessibilità dei siti web e servizi informatici;
- Multi-browser: in compatibilità con almeno i browser: Internet Explorer 9 e successivi, Firefox 28 e successivi, Chrome 24 e successivi, Safari 6 e successivi;

- Motore di ricerca full-text: permette la ricerca, sulla base della corrispondenza con specifiche parole chiave, all'interno del contenuto informativo reso accessibile dal servizio di accesso web in oggetto;
- Newsletter: permette l'invio agli utenti iscritti, di aggiornamenti e comunicazioni;
- Tag cloud: lista pesata presentata in ordine alfabetico che permette la visualizzazione di etichette cliccabili che rimandano allo specifico contenuto (alle etichette, relative agli argomenti più rilevanti, è attribuito un font più grande);
- Feed RSS/Atom: permette la distribuzione di contenuti resi accessibili dal servizio di accesso web in oggetto in formato XML compatibile con i lettori RSS/Atom.

[R.233] La piattaforma CMS deve prevedere un ambiente di pre-produzione e di produzione, quest'ultimo con funzionalità automatiche di allineamento dei contenuti in pre-produzione, a valle della validazione da parte di AgID.

[R.234] La piattaforma CMS deve essere in grado di gestire almeno le seguenti tipologie di utenze:

- **Non autenticato:** utente generico del World Wide Web (WWW);
- **Soggetti di cui ai commi a) e b) del requisito [R.13]:** utente accreditato facente parte della struttura organizzativa di un Q-ISP;
- **Fornitore dei "Servizi Applicativi" (rif. [R.185]):** utente accreditato facente parte della struttura organizzativa di un Q-ASP;
- **Gestore PEC:** utente accreditato facente parte della struttura organizzativa di un gestore PEC;
- **PA:** utente accreditato facente parte della struttura di una PA che ha aderito (o intende aderire) ai servizi SPC² (compresi i soggetti di cui all'art. 75, comma 3-bis del d.lgs. 30 dicembre 2010 n.235);

- **Soggetto sussidiario con Community Network:** utente accreditato facente parte della struttura organizzativa di una Regione o di qualsiasi altro soggetto sussidiario;
- **AGID:** utente accreditato facente parte della struttura organizzativa dell'AGID;
- **CERT-PA:** utente accreditato facente parte della struttura organizzativa dell'AGID che ha la responsabilità del CERT-PA.

[R.235] Il Fornitore deve garantire che la piattaforma CMS sia in grado di registrare le attività effettuate da ogni singola utenza descritta al requisito [R.234].

[D.7] Di seguito si riporta la descrizione delle Aree Funzionali che caratterizzano l'infrastruttura di gestione dell'Accesso Web.

Area Informativa SPC²

[R.236] Il Fornitore deve prevedere una "Area Informativa SPC²", i cui contenuti (comprese le descrizioni e documenti correlati) devono essere definiti in fase di progettazione esecutiva e corrispondere almeno ai seguenti elementi minimi:

- Informazioni sul Sistema Pubblico di Connettività e Cooperazione: contesto normativo e tecnico, documentazione pubblica della Commissione di Coordinamento, documentazione tecnico-operativa e contrattuale, etc.;
- Informazioni sulla distribuzione geografica (in termini di servizi contrattualizzati e importo economico complessivo) del SPC²;
- Catalogo dei Servizi SPC²: descrizione dei servizi delle IC-SPC, di Connettività e Applicativi, riferimenti alla documentazione di riscontro, etc.;
- IPA: descrizione delle funzionalità IPA, statistiche e link al servizio;
- Statistiche generali SPC²: aggregati statistici economico-contrattuali (es. numero di aderenti ad SPC², cardinalità dei servizi attivi, valori economici aggregati, etc.);

- Area Informativa QXN: descrizione dei requisiti, delle procedure di adesione ed attivazione del servizio IQXN; pubblicazione di documentazione tecnica, news ed eventi, contatti; link di accesso all'Area riservata per la condivisione di informazioni tra i soggetti interconnessi alla rete QXN. Nell'Area riservata devono essere disponibili almeno le seguenti informazioni:
 - a) Prefissi Infranet OPA annunciati su QXN;
 - b) Lista Domini gestiti dall'infrastruttura DNS QXN;
 - c) Procedure operative e modulistica.

[R.237] I documenti presenti nell'Area Informativa devono poter essere caricati e pubblicati secondo quanto riportato nel requisito [R.231].

Area Governance dei Servizi SPC² per i Fornitori SPC²

[R.238] Il Fornitore deve predisporre un'area "Governance dei Servizi SPC² per i Fornitori SPC²", i cui contenuti (comprese le descrizioni e documenti correlati) devono essere definiti in fase di progettazione esecutiva e corrispondere almeno ai seguenti elementi minimi:

- Gestione dei documenti: form per il caricamento dei documenti da pubblicare nell'Area Informativa SPC²;
- Gestione delle escalation: form per la richiesta di intervento a IC-SPC per la risoluzione di escalation tecniche, che interessano più fornitori, e di sicurezza attraverso il Servizio di Gestione delle Escalation;
- Gestione dei contratti: form per la compilazione, variazione e gestione dei Progetti dei Fabbisogni (configurazione di ciascun servizio e dettagli come valore contrattuale, data trasmissione, data approvazione, versione, data di attivazione, etc.) e caricamento massivo degli allegati (Piani di Attuazione), form per la ricevuta di consegna del Piano dei Fabbisogni, form per la richiesta di approvazione Progetti dei Fabbisogni alla P.A. contraente; form per la compilazione dei Contratti Esecutivi e l'eventuale firma digitale degli stessi o, in alternativa, stampa del

Contratto Esecutivo compilato per la firma analogica ed il successivo upload del Contratto stesso in versione elettronica previa acquisizione digitale del Contratto firmato analogicamente;

- Form per l'inserimento del fatturato annuale e le penali corrisposte ordinati per Amministrazione e per servizio ai sensi dell'articolo 13.4 del CQ OPA;
- Caricamento dei dati di qualità e sicurezza: manuale per l'operatore di interfacciamento con il sistema CMK (di cui al requisito [R.216]) e dashboard degli eventi di allarme sul caricamento e registro storico dei caricamenti;
- QXN – Gestione degli annunci BGP e del DNS: form per la compilazione, variazione e gestione (nell'area riservata di cui al requisito [R.236]) degli annunci BGP e delle zone DNS dei soggetti interconnessi alla QXN.

Area Governance dei Servizi SPC² per le PA

[R.239] Il Fornitore deve prevedere un' area "Governance dei Servizi SPC² per le PA", i cui contenuti (comprese le descrizioni e documenti correlati) devono essere definiti in fase di progettazione esecutiva e corrispondere almeno ai seguenti elementi minimi:

- Gestione dei contratti: form per la compilazione e la variazione dei Piani dei Fabbisogni (solo quantitativa); form per l'approvazione dei Progetti dei Fabbisogni (e di ogni loro successiva variazione derivante dalla trasmissione di una variazione ai piani dei fabbisogni) e l'eventuale firma digitale dei Contratti Esecutivi; se il contratto non è firmato digitalmente, form per l'inserimento della data di firma del contratto, digitalizzazione del Contratto e relativo Piano dei Fabbisogni; form per l'approvazione o la richiesta di modifica dei Progetti dei Fabbisogni.

- Visualizzazione delle escalation: elenco degli eventi di escalation tecniche e di sicurezza gestite tramite il Servizio di Gestione delle Escalation (cfr. §3.3) che interessano la P.A.;
- Accesso ai servizi IC-SPC: link per l'accesso ai servizi IPA e RNDT, nonché al CERT-PA.

Area Governance SPC² per AgID e Consip

[R.240] Il Fornitore deve prevedere una area “Governance SPC² per AgID e Consip”, i cui contenuti (comprese le descrizioni e documenti correlati) devono essere definiti in fase di progettazione esecutiva e corrispondere almeno ai seguenti elementi minimi:

- Documenti Area Informativa: form per il caricamento dei documenti da pubblicare nell'Area Informativa SPC²;
- Gestione dei contratti: form per l'approvazione o per la richiesta di modifica dei Piani dei Fabbisogni e dei Progetti dei Fabbisogni con annessi Piani di Attuazione; form per la creazione di report con query personalizzate per la creazione di reportistica dedicata ad AgID e Consip;
- Cruscotti ed indicatori direzionali: ambiente che consente la personalizzazione di dati storici e statistici (consistenza e caratteristiche tecniche dei servizi attivati, qualità del servizio, dati economici, etc.) da parte di AgID e Consip;

Area Reportistica dei Servizi SPC²

[R.241] Il Fornitore deve prevedere un'area “Reportistica dei Servizi SPC²”, i cui contenuti (comprese le descrizioni e documenti correlati) devono essere definiti in fase di progettazione esecutiva e corrispondere almeno ai seguenti elementi minimi:

- Reportistica relativa alla “Anagrafe Unica dei Contratti”: report statici e dinamici relativi ai dati della piattaforma AUC;
- Reportistica relativa ai Dati di Qualità e Sicurezza: report statici e dinamici relativi ai dati della piattaforma DQS;

- Reportistica Capienza Contrattuale: report statici e dinamici relativi ai valori economici dei contratti esecutivi sottoscritti da ogni singolo Fornitore SPC², con evidenza della capacità contrattuale residuale.

[R.242] La redazione, la gestione e l'aggiornamento della reportistica di cui al requisito [R.241] è a cura del Fornitore.

Area Governance dei Servizi IC-SPC

[R.243] Il Fornitore deve prevedere un'area "Governance dei Servizi IC-SPC", i cui contenuti (comprese le descrizioni e documenti correlati) devono essere definiti in fase di progettazione esecutiva e corrispondere almeno ai seguenti elementi minimi:

- Gestione dei documenti: form per il caricamento dei documenti da pubblicare nell'Area Informativa SPC²;
- Catalogo dei Servizi IC-SPC: descrizione dei servizi IC-SPC, modalità di adesione, documentazione tecnico-contrattuale, di riscontro, etc.;
- Gestione dei contratti: form per la gestione automatica dei contratti sottoscritti tra il gestore dei servizi IC-SPC e i soggetti sottoscrittori (compilazione contratti e piani fabbisogni, variazione fabbisogni, etc.);
- Gestione delle escalation: form per gestione delle richieste di intervento a IC-SPC per la risoluzione di escalation tecniche e di sicurezza attraverso il Servizio di Gestione delle Escalation.

Area Reportistica dei Servizi IC-SPC

[R.244] Il Fornitore deve prevedere un'area "Reportistica dei Servizi IC-SPC", i cui contenuti (comprese le descrizioni e documenti correlati) devono essere definiti in fase di progettazione esecutiva e corrispondere almeno ai seguenti elementi minimi:

- Reportistica IC-SPC: report statici e dinamici su consistenza, utilizzo, qualità, sicurezza dei servizi IC-SPC erogati dal Fornitore;

- Reportistica penali IC-SPC-AGID: reportistica delle penali dovute dal Fornitore ad AGID e ai soggetti sottoscrittori, relative ai servizi IC-SPC;

[R.245] La redazione, la gestione e l'aggiornamento della reportistica di cui al requisito [R.244] è a cura del Fornitore.

Matrice di visibilità delle Aree Informative, di Governance e di Reportistica

[R.246] Il Fornitore deve consentire agli utenti definiti in [R.234] l'accesso alle differenti Aree secondo due classificazioni di privilegi:

- **L:** abilitazione in lettura;
- **S:** abilitazione in lettura e scrittura.

Fornitori e PA avranno comunque accesso ai soli dati contrattuali, di qualità e sicurezza, relativi ai contratti da essi sottoscritti.

[D.8] A titolo esemplificativo e non esaustivo nella seguente tabella è rappresentata una classificazione degli utenti per le Aree precedentemente individuate:

	Fornitore IC-SPC*	Utente non autenticato	Fornitore SPC ² Connettività	Fornitore dei "Servizi Applicativi"	PA	Soggetto sussidiario	AGID/Consip	CERT-PA
Area informativa SPC ²	S	L	S	S	L	L	S	
Area Governance dei Servizi SPC ² per i Fornitori	L*		S	S			L	
Area Governance dei Servizi SPC ² per le PA	L*				S		L	
Area Governance dei Servizi SPC ² per AgID e Consip	L*						S	

Area Reportistica dei Servizi SPC²	S*		S	S	L		L	L
Area Governance dei Servizi IC SPC²	S		S	S		S	L	
Area Reportistica dei Servizi IC SPC²	S		L	L	L	L	L	L

Tabella 5

** Il Fornitore IC-SPC potrà accedere alle aree indicate in tabella a soli fini di gestione*

ed amministrazione della piattaforma

[R.247] Gli utenti abilitati in scrittura dovranno essere abilitati esclusivamente alle parti di propria competenza di ciascuna Area prevista dalla suddetta tabella.

Modalità di accreditamento e di gestione delle utenze per l'Accesso Web SPC

[R.248] Il Fornitore deve garantire, per ciascuna utenza di cui al requisito [R.234], la seguente differenziazione:

- 1) Utenza Master;
- 2) Utenza Slave.

[R.249] Relativamente alle utenze Master, di cui al punto 1 del requisito [R.248], il Fornitore deve garantirne l'accREDITamento diretto con le modalità descritte al requisito [R.252].

[R.250] Il Fornitore deve predisporre affinché le utenze Master, di cui al punto 1 del requisito [R.248], attraverso una apposita web form di accREDITamento, possano accREDITare fino a 10 (dieci) utenze Slave (associate all'utenza Master).

[R.251] Il Fornitore deve garantire che le utenze di cui al requisito [R.234] di tipo Slave, abbiano accesso alle stesse aree offerte dal Servizio di Accesso Web SPC previste per le utenze Master che le hanno accREDITate, eccetto la web form di accREDITamento di cui al requisito [R.250].

[R.252] L'accREDITamento diretto delle utenze Master di cui al requisito [R.234] deve essere garantito dal Fornitore attraverso due modalità:

- a) Modalità di accREDITamento per utenze accREDITate su IPA;
- b) Modalità di accREDITamento per utenze non accREDITate su IPA.

[R.253] Il Fornitore deve predisporre affinché la modalità di accREDITamento diretta a) di cui al [R.252], avvenga attraverso una web form che garantisca l'accREDITamento automatico dei soggetti per i quali devono essere già presenti le seguenti informazioni su IPA:

- Amministrazione di appartenenza;
- UO (Unità Organizzativa) di appartenenza;
- Servizio offerto denominato "Servizio di Gestione dei Contratti SPC" oppure "Servizio Unità Locale di Sicurezza SPC";

- Nome, cognome e indirizzo e-mail (ordinario o PEC) del responsabile dell'UO a cui è associato il servizio di cui al punto precedente.

[R.254] I soggetti, per i quali i dati di cui sopra non sono disponibili in IPA, non potranno essere accreditati dal Fornitore con la modalità diretta a) di cui al [R.252], senza aver prima integrato/aggiornato i propri dati secondo le modalità previste per IPA.

[R.255] La *web form* di cui al requisito [R.253], deve prevedere almeno i seguenti campi popolati da IPA:

- Menu a discesa per la selezione dell'Amministrazione di appartenenza;
- Menu a discesa per la selezione della UO di appartenenza dell'Amministrazione;
- Menu a discesa per la selezione del servizio offerto (uno tra i servizi offerti di cui al requisito [R.253]).

[R.256] Al termine della corretta compilazione della *web form* di cui al requisito [R.253], il Fornitore deve inviare una e-mail (PEC), contenente le credenziali per l'Accesso Web SPC, all'indirizzo di riferimento del responsabile dell'UO che sta effettuando la richiesta di accreditamento.

[R.257] Il Fornitore deve predisporre affinché la modalità di accreditamento diretta b) di cui al [R.252] sia effettuata alla ricezione (tramite e-mail o PEC) di specifica richiesta proveniente da AgID contenente almeno Nome, Cognome e indirizzo e-mail al quale inviare le credenziali per l'accesso al servizio.

4 Servizi di Supporto all'Operatività (SSOP)

[R.258] Nell'ambito dei servizi oggetto della presente gara, il Fornitore deve erogare anche i servizi di supporto che comprendono le seguenti attività:

- Installazione, attivazione, cessazione e variazione dei servizi e delle relative componenti (Procurement e Change Management);
- Supervisione della rete (Network Monitoring) e gestione degli apparati;
- Configurazione, monitoraggio, registrazione e attivazione delle procedure di Incident e Problem Management relativamente a eventi/allarmi di sicurezza;
- Adozione delle misure di sicurezza sulle infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato;
- Supporto tecnico alla gestione dei malfunzionamenti (Trouble Ticket e Fault Management);
- Registrazione e controllo di utenti e dispositivi che accedono alle risorse di rete e di sistema;
- Distribuzione del software e eventuali aggiornamenti (Release Management) e gestione centralizzata delle configurazioni (Configuration Management);
- Analisi delle prestazioni del servizio (Performance Management);
- Verifica del corretto dimensionamento complessivo del sistema, tuning delle configurazioni degli apparati e attività di Planning e Capacity Management;
- Produzione periodica di reportistica (Reporting) per controllo dei SLA definiti (SLA Management).

[R.259] La reportistica deve essere prodotta ed inviata ad AgID nelle modalità e nei tempi definiti nell'appendice SLA e penali;

[R.260] Per la realizzazione dei servizi di cui al requisito [R.258] il Fornitore deve dotarsi delle seguenti **strutture di supporto**:

- **NOC (Network Operating Center):** Centro di Gestione di rete;

- **SOC (Security Operating Center):** Centro di Gestione della sicurezza;
- **AOC (Application Operating Center):** Centro di Gestione delle applicazioni/sistemi;
- **Service Desk (SEDE):** integrato con le piattaforme di erogazione dei servizi IC, assicura nel complesso i livelli di servizio contrattualizzati;

[R.261] Per la realizzazione dei servizi di cui al requisito [R.258] il Fornitore deve dotarsi dei seguenti strumenti di supporto non necessariamente dedicati alle Infrastrutture Condivise SPC:

- **Infrastrutture Condivise Data Base (ICDB):** il Data Base delle Infrastrutture Condivise SPC contenente tutte le informazioni relative ai sistemi e servizi nell'ambito di IC-SPC;
- **Piattaforma di Trouble Ticket Management (PTTM):** piattaforma per la gestione, il monitoraggio e il tracciamento di tutte le attività mediante trouble ticket;
- **Sistema di Rendicontazione e Fatturazione (SIRF):** cruscotto per la visualizzazione dei dati di qualità e di fatturazione dei servizi.

[R.262] Il Fornitore deve garantire che i locali **Data Center** che ospiteranno i sistemi per l'erogazione dei servizi, ivi compresi quelli definiti in [R.4] posseggano i seguenti requisiti minimi:

- Impianto di condizionamento, opportunamente dimensionato per gli apparati ed il personale ivi operante;
- Sistemi di continuità elettrica (UPS, gruppi elettrogeni, ecc.);
- Sistemi di rilevazione fumi ed impianto antincendio;
- Sistemi anti-allagamento: devono essere previste 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: deve essere predisposto un sistema anti-intrusione integrato con un impianto di video sorveglianza.

Dovranno essere, inoltre, posizionate 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: deve essere garantito 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.

[R.263] Il Fornitore deve garantire che i componenti coinvolti nell'erogazione dei differenti servizi siano ridondanti in modo da eliminare *single point of failure*.

[R.264] Il Fornitore deve garantire che su tutte le infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato siano adottate le seguenti misure di controllo 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 e dei sistemi con l'obiettivo di intervenire, anche proattivamente, a seguito di problemi di carico o del riconoscimento di potenziali attacchi e per la rimozione delle criticità riscontrate;
- 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 e resi disponibili al CERT-PA secondo le modalità indicate da AgID. 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.

[R.265] Il Fornitore deve garantire che su tutte le infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato siano adottate le seguenti misure di carattere generale:

- 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 e s.m.i.);
- Disposizione di un'organizzazione per la gestione della sicurezza dell'infrastruttura, secondo gli attuali standard di riferimento;
- Disposizione, nei punti di ingresso alle proprie infrastrutture utilizzate per l'erogazione dei servizi, di sistemi di controllo e filtraggio del traffico, di verifica e prevenzione di intrusioni e della verifica dell'assenza di virus e codice malevolo;
- Garanzia di tempestivo aggiornamento, con applicazione delle patch, del software/firmware degli apparati di rete e di sistema nel perimetro dei servizi oggetto del presente capitolato;
- Implementazione di un meccanismo centralizzato per l'autenticazione, l'autorizzazione e la tracciatura degli accessi sugli apparati di rete e di sistema nel perimetro dei servizi oggetto del presente capitolato.

[R.266] Il Fornitore deve garantire che su tutte le infrastrutture utilizzate per l'erogazione dei servizi oggetto del presente Capitolato siano adottate le seguenti misure organizzative:

- Analisi dei rischi su base sistematica, almeno con cadenza annuale. Tale analisi deve inoltre essere ripetuta a seguito di attacchi o incidenti gravi di sicurezza o per variazioni significative dell'architettura;
- Schedulazione di attività periodiche 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.

4.1 Organizzazione

[R.267] Il Fornitore deve dotarsi di una struttura organizzativa per la **gestione tecnica ed operativa** dei servizi di cui al [R.1] che prevede almeno le seguenti strutture:

- a) Direzione Tecnica affidata alla responsabilità di un “**Direttore Tecnico IC-SPC**”;
- b) **Unità Locale di Sicurezza SPC²**.

[R.268] Il Direttore Tecnico IC-SPC ha:

- a) L'obbligo di partecipare al Comitato di Direzione Tecnica previsto dalla gara a procedura ristretta per l'affidamento dei servizi di connettività nell'ambito del Sistema Pubblico di Connettività (CIG 5133642F61 - ID SIGEF 1367);
- b) L'obbligo di partecipare al Comitato Tecnico QXN;
- c) L'obbligo di partecipare al Comitato Operativo IC-SPC;
- d) Il compito di garantire l'operatività tecnica della rete QXN e di tutti i servizi oggetto di fornitura della presente gara.

[R.269] L'Unità Locale di Sicurezza SPC² è presieduta dal Direttore Tecnico IC-SPC e svolge i seguenti compiti:

- a) garantire la realizzazione ed il mantenimento dei livelli di sicurezza previsti dal Sistema Pubblico di Connettività e Cooperazione;
- b) garantire che la politica di sicurezza presso la propria organizzazione sia conforme agli indirizzi e alle politiche di sicurezza definiti dalla Commissione di Coordinamento SPC²;
- c) interagire con AgID per raccogliere, aggregare e predisporre nel formato richiesto le informazioni necessarie per verificare il livello di sicurezza del SPC²;
- d) notificare ad AgID ed al CERT-PA, secondo le modalità stabilite e comunicate da AgID, eventuali incidenti informatici o situazioni di criticità o vulnerabilità della QXN e delle infrastrutture SPC² preposte all'erogazione di servizi condivisi;
- e) adottare le necessarie misure volte a limitare il rischio di attacchi informatici ed eliminare eventuali vulnerabilità della rete, causate dalla violazione e utilizzo illecito di sistemi o infrastrutture della pubblica amministrazione.

[R.270] In conformità al D.P.C.M. del 1° Aprile 2008 “Regole tecniche e di sicurezza per il funzionamento del Sistema Pubblico di Connettività” (G.U. n. 144 del 21

Giugno 2008), i compiti della Unità Locale di Sicurezza SPC² devono essere svolti dal SOC.

- [R.271] Il Fornitore deve nominare, all'interno della Unità Locale di Sicurezza SPC² un **Responsabile Operativo della Sicurezza** che riporta al Direttore Tecnico IC-SPC e coordina l'operatività dell'Unità Locale di Sicurezza SPC², fungendo da punto di contatto prioritario per tutte le problematiche di sicurezza che interessano l'infrastruttura della rete QXN, dei Servizi di Governance e per l'Interoperabilità delle Applicazioni. Il Responsabile Operativo della sicurezza potrà avvalersi di sostituti i cui nominativi dovranno essere preventivamente comunicati all'AgID.

4.2 Sicurezza

Sicurezza Fisica

- [R.272] Gli apparati attivi di rete ed i server che erogano i servizi descritti nel presente Capitolato devono essere compartimentati mediante armadi di cablaggio con chiusura a chiave; in particolare gli apparati deputati all'erogazione di servizi critici all'interno del Data Center come la generazione delle chiavi crittografiche ed i certificati digitali devono risiedere all'interno di tali locali in ambienti fisicamente separati e ad accesso riservato e controllato con strumenti di rilevazione idonei.
- [R.273] La rete di interconnessione interna (LAN) dei data center utilizzata dal Fornitore per connettere i sistemi con cui vengono erogati i servizi oggetto della presente gara deve essere dedicata esclusivamente a tali servizi e su tale rete saranno attestati tutti gli apparati che comporranno il sistema; tale rete deve essere dotata di sistemi di protezione firewall, IDS e antivirus.
- [R.274] Deve essere predisposto un sistema di segnalazione degli allarmi di tipo locale o remoto.
- [R.275] Deve essere garantito un sistema di continuità elettrica con opportune ridondanze e coerente con i livelli di servizio definiti.
- [R.276] Il Fornitore deve utilizzare un registro delle visite dei data center curandone la conservazione per tutta la durata contrattuale.

Sicurezza Logica

- [R.277] Il sistema operativo degli elaboratori utilizzati per l'erogazione dei servizi, deve assicurare:

- L'univoca identificazione ed autenticazione degli utenti;
- La protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- La garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- La registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

[R.278] Le patch che risolvano problematiche di sicurezza critiche per i server esposti in Internet devono essere installate tempestivamente e successivamente deve essere inviata opportuna relazione tecnica ad AgID.

[R.279] Per ogni installazione relativa all'infrastruttura di ciascun servizio, deve essere prodotta una checklist di sicurezza da utilizzarsi in fase di collaudo; tale checklist dovrà essere approvata da AgID.

[R.280] Il Fornitore deve progettare, concordandole con AgID, ed eseguire delle attività di verifica della sicurezza (come ad esempio penetration-test) da realizzare con cadenza quadrimestrale, ed aventi ad oggetto, per ogni quadrimestre, il 50% dei servizi oggetto di gara (rif. [R.1]), tra cui sempre l'IPA e, per il resto, a rotazione concordata con AgID. Le attività di verifica della sicurezza devono essere svolte in modo da minimizzare l'impatto sul servizio in esercizio. Il Fornitore si impegna comunque ad autorizzare lo svolgimento di ulteriori test discrezionali di impenetrabilità da parte di AGID. Nel caso in cui le attività di verifica e i test di cui sopra evidenzino carenze di sicurezza, il fornitore dovrà provvedere alla correzione di dette carenze rispetto alle specifiche tecniche di sicurezza presenti nel capitolato, con le tempistiche indicate nell'appendice "SLA e penali".

[R.281] Il mantenimento della sicurezza nel tempo è soggetto ad audit periodici. In particolare, il Fornitore si impegna a far eseguire annualmente, a proprie spese, un approfondito audit sul sistema di sicurezza, condotto da una primaria società specializzata scelta dal Fornitore previa approvazione di AGID. AGID potrà, con un preavviso di 20 (venti) giorni solari, richiedere ulteriori attività di auditing secondo modalità concordate con il Fornitore.

Sicurezza Organizzativa

[R.282] Il Fornitore deve garantire che tutte le risorse hardware o software necessarie all'erogazione dei servizi del presente Capitolato siano gestite solo da personale univocamente individuato.

[R.283] Il Fornitore deve rendere 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;
- Accesso fisico delle persone ai locali contenenti apparati;
- Regole per l'accesso da parte di personale esterno (fornitori, addetti alla manutenzione, visitatori, ecc.);
- Gestione degli strumenti per l'accesso ad eventuali casseforti ed armadi blindati (combinazioni delle casseforti, chiavi degli armadi, ecc.);
- Gestione degli archivi cartacei (regole per la conservazione, modalità di consultazione, eventuale registrazione degli accessi, ecc.);
- Gestione di situazioni anomale;
- Ripristino dell'erogazione di energia elettrica in caso di interruzione;
- Procedure di backup e di restore;
- Procedure di escalation.

[R.284] **Disaster Recovery.** Il Fornitore deve progettare ed implementare una soluzione tecnica che, qualora si verificano eventi eccezionali che ne impediscano il funzionamento, consenta il ripristino dell'erogazione dei servizi entro il termine massimo di 10 giorni solari ed assicuri la messa in sicurezza dei dati entro massimo 30 ore dalla loro acquisizione e/o produzione.

[R.285] AgID si riserva la possibilità di effettuare sopralluoghi nei locali ospitanti sistemi e apparati coinvolti nell'erogazione dei servizi con un preavviso minimo di 3 giorni lavorativi.

4.3 Strutture di supporto

Network Operating Center (NOC)

[R.286] Il Fornitore deve predisporre un NOC, non necessariamente dedicato alle Infrastrutture Condivise SPC, che deve assolvere alle seguenti funzioni:

- Gestione della rete, con monitoraggio real-time di ogni servizio di rete allo scopo di determinare potenziali problemi e assicurare che vengano rispettati i livelli di servizio contrattualizzati;
- Gestione centralizzata delle configurazioni di tutti gli apparati di rete che rientrano nel perimetro dei servizi erogati e di supporto;
- Gestione degli allarmi e dei malfunzionamenti delle componenti del servizio ed attivazione delle procedure di Incident e Problem Management;
- Verifica del corretto dimensionamento complessivo del sistema di rete e attività di capacity planning a seguito della pianificazione e propedeutiche alla implementazione di modifiche consistenti o all'introduzione di nuovi servizi;
- Monitoraggio del grado di occupazione delle risorse trasmissive;
- Monitoraggio dei livelli di servizio e calcolo statistiche;
- Supporto alla produzione di reportistica.

[R.287] Il NOC deve essere operativo per 24 ore al giorno, per 7 giorni alla settimana e per 365 giorni l'anno.

[R.288] Il sistema di gestione della rete deve essere basato su architetture che garantiscano la sicurezza, integrità e confidenzialità delle comunicazioni e conformi agli standard applicabili.

[R.289] Il NOC deve acquisire il Tempo Ufficiale di Rete SPC² di cui al §1.10 e utilizzarlo come riferimento temporale assoluto ai fini della marcatura con "time stamp" dei log e dei trouble ticket, nonché per tutte le altre funzioni di gestione della rete che richiedono un riferimento temporale.

Security Operating Center (SOC)

[R.290] Il Fornitore deve realizzare e gestire un SOC, non necessariamente dedicato alle Infrastrutture Condivise SPC, che deve assolvere alle seguenti funzioni:

- Monitoraggio continuo e real-time del funzionamento dei servizi di sicurezza al fine di determinare potenziali problemi e

assicurare che vengano rispettati i livelli di servizio contrattualizzati;

- Registrazione di tutti gli eventi riguardanti la sicurezza;
- Gestione degli allarmi e dei malfunzionamenti delle componenti del servizio ed attivazione delle procedure di Incident e Problem Management;
- Relativamente agli aspetti di sicurezza: gestione delle configurazioni, patching e hardening di tutti gli apparati e sistemi ICT che rientrano nel perimetro dei servizi erogati e di supporto;
- Verifica del corretto dimensionamento complessivo del sistema di sicurezza e attività di capacity planning a seguito della pianificazione e propedeutiche alla implementazione di modifiche consistenti o all'introduzione di nuovi servizi;
- Supporto alla produzione di reportistica dei servizi di sicurezza, degli incidenti verificatisi nonché delle relative operazioni di correzione effettuate.

[R.291] Il SOC deve essere operativo per 24 ore al giorno e per 365 giorni l'anno.

[R.292] Il trasferimento di dati critici/sensibili, quali ad esempio configurazioni di sicurezza, tra apparati gestiti e sistema di gestione del Fornitore, deve essere adeguatamente protetto con opportuni meccanismi di sicurezza volti a preservare la confidenzialità delle informazioni (es. SSH, IPsec).

[R.293] Le infrastrutture tecnologiche del SOC devono essere realizzate nel pieno rispetto e conformità alla normative vigenti in tema di sicurezza fisica e logica, best practice e standard applicabili.

[R.294] Il SOC deve acquisire il Tempo Ufficiale di Rete SPC² di cui al §1.10 e utilizzarlo come riferimento temporale assoluto ai fini della marcatura con "time stamp" dei log e dei trouble ticket, nonché per tutte le altre funzioni di gestione della rete che richiedono un riferimento temporale.

Application Operating Center (AOC)

[R.295] Il Fornitore deve realizzare e gestire un AOC, non necessariamente dedicato alle Infrastrutture Condivise SPC, che deve assolvere alle seguenti funzioni:

- Gestione delle applicazioni e dei sistemi, con monitoraggio real-time di ogni servizio allo scopo di determinare potenziali problemi e assicurare che vengano rispettati i livelli di servizio contrattualizzati;
- Gestione centralizzata delle configurazioni di tutti i sistemi che rientrano nel perimetro dei servizi erogati e di supporto;
- Gestione degli allarmi e dei malfunzionamenti delle componenti del servizio ed attivazione delle procedure di Incident e Problem Management;
- Verifica del corretto dimensionamento complessivo dei sistemi e attività di capacity planning a seguito della pianificazione e propedeutiche alla implementazione di modifiche consistenti o all'introduzione di nuovi servizi
- Monitoraggio del grado di occupazione delle risorse elaborativo;
- Monitoraggio dei livelli di servizio e calcolo statistiche;
- Supporto alla produzione di reportistica.

[R.296] L'AOC deve essere operativo per 24 ore al giorno per 365 giorni l'anno.

[R.297] Il sistema di gestione delle applicazioni e dei sistemi deve essere basato su architetture che garantiscano la sicurezza, integrità e confidenzialità delle informazioni e conformi agli standard applicabili.

[R.298] L'AOC deve acquisire il Tempo Ufficiale di Rete SPC² di cui al §1.10 e utilizzarlo come riferimento temporale assoluto ai fini della marcatura con "time stamp" dei log e dei trouble ticket, nonché per tutte le altre funzioni di gestione delle applicazioni e dei sistemi che richiedono un riferimento temporale.

Service Desk (SEDE)

[R.299] Il Fornitore deve garantire che il servizio Service Desk gestisca tutti gli incidenti, problemi e richieste di servizio inerenti tutti i servizi erogati dalle IC-SPC, deve rappresentare l'interfaccia unica per i seguenti processi:

- Incident Management;
- Problem Management;

- Configuration Management;
- Change Management;
- Release Management;
- Service-Level Management;
- Availability Management;
- Capacity Management;
- Service Continuity Management;
- Security Management.

[R.300] Il Fornitore dovrà rendere disponibile un punto unico di contatto per il servizio di cui al Requisito [R.299], raggiungibile attraverso:

- Un numero unico telefonico gratuito (numero verde a tariffa omnicomprendiva a carico del Fornitore);
- Posta elettronica;
- Interfaccia web;
- Fax.

[R.301] Il servizio di cui al requisito [R.299] deve essere erogato in lingua italiana.

[R.302] Il servizio deve essere in grado di gestire almeno le seguenti tipologie di utenze:

- Soggetti sottoscrittori del Servizio di Interconnessione QXN (IQXN);
- Utenti del Servizio di Gestione dell'Accesso Web (SGAW), ad esclusione della categoria "Utente non autenticato";

[R.303] Per ciascun soggetto di cui al requisito [R.302] il Fornitore deve garantire che il servizio di Service Desk sia in grado di gestire le seguenti attività:

- Punto informazioni: fornisce informazioni generali (funzionalità, modalità di sottoscrizione, etc.) riguardanti i servizi IC-SPC erogati;

- Gestione degli incidenti/problemi: a fronte di guasti e/o problematiche di funzionamento dei servizi IC-SPC erogati, ne cura la risoluzione e le relazioni con i fruitori, ivi compresi eventuali servizi di supporto alle attività dell'IPA;
- Gestione attivazioni/disattivazioni e configurazioni: gestisce l'attivazione (o la disattivazione) di utenze legate ai servizi IC-SPC, gestisce inoltre anche eventuali richieste di cambio di configurazioni.

[R.304] Il Service Desk deve alimentare e gestire una Knowledge Base contenente un elenco delle soluzioni alle problematiche note in modo da poter applicare direttamente la soluzione o il workaround senza procedere ad escalation verso i livelli tecnici superiori.

[R.305] Il servizio Service Desk dovrà essere disponibile per 24 ore al giorno, per 365 giorni l'anno.

4.4 Strumenti di supporto

Infrastrutture Condivise DataBase (ICDB)

[R.306] Il Fornitore deve disporre di un **sistema di basi dati (Infrastrutture Condivise Data Base, ICDB)** per supportare le attività di NOC, SOC, AOC e Service Desk.

[R.307] L'ICDB deve svolgere le funzioni di **database delle configurazioni (Configuration Management Data Base, CMDB)** per gestire e controllare tutte le configurazioni hardware e software degli apparati utilizzati per l'erogazione dei servizi, 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 di un report generale delle configurazioni;
- La pianificazione delle attività di gestione e di aggiornamento dei sistemi.

[R.308] L'ICDB deve svolgere le funzioni del **database del NOC** e contenere informazioni su:

- Ubicazione, tipologia e configurazione degli apparati utilizzati;
- Misurazioni utilizzate per il calcolo dei livelli di servizio;
- Log delle richieste di intervento pervenute dal Service Desk;
- Log dei trouble ticket relativi a incidenti, richieste di servizio e di variazione delle configurazioni dei sistemi;
- Classificazione eventi, allarmi e malfunzionamenti;
- Dati di riscontro della qualità.

[R.309] L'ICDB deve svolgere le funzioni del **database del SOC** e contenere informazioni su:

- Ubicazione, tipologia e configurazione dei sistemi di sicurezza utilizzati;
- Policy configurate per ciascun sistema;
- Misurazioni utilizzate per il calcolo dei livelli di servizio;
- Log delle richieste di intervento pervenute dal Service Desk;
- Log dei trouble ticket relativi a incidenti di sicurezza, richieste di servizio e di variazione delle configurazioni dei sistemi di sicurezza;
- Classificazione eventi, allarmi e malfunzionamenti;
- Dati di riscontro della qualità.

[R.310] L'ICDB deve svolgere le funzioni del **database dell'AOC** e contenere informazioni su:

- Ubicazione, tipologia e configurazione dei sistemi utilizzati;
- Misurazioni utilizzate per il calcolo dei livelli di servizio;
- Log delle richieste di intervento pervenute dal Service Desk;
- Log dei trouble ticket relativi a incidenti, richieste di servizio e di variazione delle configurazioni dei sistemi;

- Classificazione eventi, allarmi e malfunzionamenti;
- Dati di riscontro della qualità.

Piattaforma di Trouble Ticket Management (PTTM)

- [R.311] Il Fornitore, nell'ambito della servizio di Service Desk, deve disporre di una **Piattaforma di Trouble Ticket Management (PTTM)** che garantisca la gestione, il monitoraggio e il tracciamento di tutte le attività.
- [R.312] La PTTM deve prevedere meccanismi di apertura dei ticket relativi a disservizi o malfunzionamenti dei servizi erogati dalle IC-SPC, in modalità proattiva, ossia anche in assenza di esplicite segnalazioni pervenute al punto unico di contatto.
- [R.313] Il Fornitore deve storicizzare le informazioni relative ai TT in modo da consentire l'analisi successiva sino al livello del singolo disservizio e fruitore dei servizi SPC (AgID o Fornitore SPC Qualificato).
- [R.314] La PTTM dovrà essere in grado di tracciare almeno le informazioni minime seguenti:
- Identificazione del TT;
 - Modalità di ricezione (automatico, telefono, mail, web etc.);
 - Data ed orario di apertura;
 - Soggetto che ha richiesto l'intervento;
 - Elenco e numero di elementi complessivamente coinvolti dal malfunzionamento;
 - Descrizione del problema;
 - Livello di severità del malfunzionamento;
 - Riferimenti operativi coinvolti nel caso specifico;
 - Smistamento alle strutture operative qualora non sia possibile fornire la soluzione;
 - Eventuali strutture terze coinvolte;
 - Diagnosi del problema;
 - Descrizione della soluzione;

- Data ed orario di chiusura.

Sistema di Rendicontazione e Fatturazione (SIRF)

- [R.315] Il sistema di rendicontazione e fatturazione è rivolto ai soggetti sottoscrittori dei Contratti Attuativi con le IC-SPC e ad AgID, con lo scopo di rendere disponibili, attraverso apposita reportistica, i dati relativi all'erogazione e fruizione dei servizi oggetto del presente Capitolato e consentire il controllo e la verifica degli importi da fatturare da parte dei soggetti di cui sopra.
- [R.316] Il Fornitore deve realizzare ed attivare, dall'avvio dell'erogazione dei servizi, una piattaforma per la rendicontazione dei dati di qualità e di fatturazione dei Servizi IC-SP, integrata con il Servizio di Gestione dell'Accesso Web (cfr. §3.4).
- [R.317] La piattaforma di cui al requisito [R.316] deve garantire almeno le seguenti funzionalità:
- Monitoraggio, in tempo reale, dei servizi contrattualizzati attraverso opportuni quadri sinottici che consentano una tempestiva percezione dello stato dei servizi;
 - Verifica dei livelli di servizio e calcolo di statistiche, per tutti i servizi contrattualizzati;
 - Consuntivazione dei servizi erogati;
 - Log dei trouble ticket gestiti dal Service Desk;
 - Consultazione diretta delle Base Dati relative alle risorse di rete e di sicurezza nel perimetro dei servizi erogati, consentendo la generazione guidata di report, grafici, e query complesse;
 - Funzionalità di esportazione dei dati, secondo formati standard preventivamente approvati con AgID, contenuti nella porzione di Base Dati relativa alle risorse di rete e di sicurezza nel perimetro dei servizi erogati.

4.5 Servizi di sviluppo

- [R.318] I servizi di sviluppo, ovvero:
- Le attività di manutenzione correttiva

- Le attività di manutenzione adeguativa ed evolutiva
- La realizzazione degli applicativi richiesti nel presente capitolato tecnico (ad es. per i servizi RNDT, SGAC)

devono essere effettuati secondo i criteri di seguito descritti.

[R.319] I servizi di sviluppo devono utilizzare metodologie in grado di minimizzare i rischi di sicurezza e le vulnerabilità del codice.

[R.320] Le attività di manutenzione correttiva dovranno essere svolte secondo un processo che preveda almeno le seguenti fasi:

- Problem determination;
- Problem solving;
- Analisi dell'impatto sul sistema esistente;
- Pianificazione dei rilasci;
- Progettazione;
- Sviluppo e testing nell'ambiente di collaudo/pre-esercizio;
- Rilascio in esercizio;
- Aggiornamento della relativa documentazione.

[R.321] Le attività di manutenzione adeguativa ed evolutiva e la realizzazione degli applicativi richiesti nel presente capitolato tecnico dovranno essere svolte secondo un processo che preveda almeno le seguenti fasi:

- Analisi dei requisiti (tecnici, funzionali e non funzionali);
- Consolidamento dei requisiti;
- Analisi dell'impatto sul sistema esistente;
- Pianificazione dei rilasci;
- Progettazione;
- Sviluppo e testing nell'ambiente di collaudo/pre-esercizio;
- Rilascio in esercizio;
- Aggiornamento della relativa documentazione.

[R.322] Gli interventi di realizzazione degli applicativi richiesti nel presente capitolato tecnico e la manutenzione correttiva saranno compresi nella valutazione economica “a corpo” dei singoli servizi.

[R.323] Gli interventi di manutenzione adeguativa ed evolutiva sono previsti per i servizi RNDT, IPA, IGPEC e per i Servizi di Governance, saranno gestiti in **modalità progettuale**.

[R.324] La **modalità progettuale** prevede che gli interventi e la relativa pianificazione siano attuati secondo un processo che sarà definito in funzione della tipologia dell'intervento medesimo. L'attività viene misurata sulla base dello stato di avanzamento lavori, in funzione della pianificazione definita e concordata con AgID. Ogni processo comprenderà una **fase di definizione** necessaria alla pianificazione dell'intervento, che il Fornitore effettuerà entro:

- 7 giorni solari in caso di interventi qualificati come “urgenti” da AgID
- 30 giorni solari in caso di interventi qualificati come “non urgenti” da AgID

e che avrà come prodotto il **Piano di Lavoro dell'Intervento** che dovrà essere approvato formalmente da AgID.

[R.325] Il **Piano di Lavoro dell'Intervento** deve comprendere almeno:

- Il **gantt** con la pianificazione degli interventi e dei rilasci
- La descrizione dei **deliverable**
- Una **matrice RACI** che identifichi con chiarezza il team di lavoro ed i reciproci ruoli e responsabilità all'interno del Fornitore evidenziando anche il ruolo di AgID
- La **stima** prevista delle risorse professionali coinvolte e del costo dell'intervento

[R.326] La regolamentazione progettuale (pianificazione e rendicontazione) e contrattuale è in “**giorni/persona**”: il calcolo del corrispettivo per ogni intervento avverrà sulla base di quanto approvato da AgID nel Piano di Lavoro dell'Intervento di cui al requisito [R.325].

[R.327] La fatturazione del suddetto corrispettivo avverrà a seguito dell'accettazione dei deliverable da parte di AgID.

- [R.328] L'ammontare economico consuntivato per la totalità degli interventi di manutenzione adeguativa ed evolutiva non potrà eccedere, rispettivamente per i servizi RNDT, IPA, IGPEC e per i Servizi di Governance, quanto riportato ai requisiti [R.149], [R.162], [R.183] e [R.203].

5 Modalità di attivazione dei servizi

5.1 Progetto Esecutivo

- [R.329] Il Fornitore, entro 60 giorni solari dalla stipula del contratto, deve inviare a AgID a mezzo PEC un documento denominato “**Progetto Esecutivo**”, nel quale formulerà la proposta tecnica dettagliata per l’erogazione dei servizi richiesti, coerente con le specifiche del presente Capitolato e dei Progetti presentati nella Relazione Tecnica.
- [R.330] Il “Progetto Esecutivo” deve contenere informazioni di dettaglio delle soluzioni tecniche e progettuali utilizzate per la realizzazione dell’infrastruttura e dei servizi oggetto della presente gara, ricorrendo anche all’ausilio di schemi logici e funzionali.
- [R.331] Il Progetto Esecutivo è sottoposto ad approvazione da parte di AgID, che potrà richiedere, a mezzo PEC, variazioni e/o integrazioni. In tal caso, il Fornitore dovrà consegnare ad AgID, sempre a mezzo PEC, il Progetto Esecutivo che recepisca le variazioni/integrazioni richieste da AgID, entro 20 giorni solari dall’invio della richiesta al Fornitore.
- [R.332] Il Progetto Esecutivo di cui al requisito [R.329] deve essere costituito, per ciascuna categoria di servizi IC-SPC (IQXN, SIA, SGOV e SSOP) erogati dal Fornitore, da:
1. **Piano di attivazione:** contenente l’elenco delle attività/fasi previste con relativo piano temporale, le modalità di presentazione ed approvazione dei SAL (Stato di Avanzamento Lavori), il gantt completo, l’organizzazione completa del Project Management Office e dei suoi processi, le soluzioni di roll-back in caso di eventuali criticità in fase di migrazione e i piani di contingency
 2. **Specifiche esecutive:** contenente le specifiche di dettaglio della progettazione, realizzazione ed erogazione del servizio con la descrizione di tutte le unità funzionali di cui è composto (architettura, sistemi utilizzati, dimensionamento, ecc.) e le modalità di gestione, ivi compresa la sicurezza e le metodologie e le tecniche utilizzate per la misurazione dei parametri previsti nell’appendice “Livelli di Servizio e Penali”, ed in particolare:
 - a) **Servizi di Interconnessione QXN:**
 - Descrizione di dettaglio dell’infrastruttura, architettura prescelta, configurazioni hardware e software di tutte le componenti utilizzate ai fini dell’erogazione dei servizi IQXN, dimensionamento e soluzioni di scalabilità;
 - b) **Servizi di Interoperabilità delle Applicazioni:**

- Descrizione di dettaglio dell'infrastruttura di elaborazione, architettura prescelta, caratteristiche tecniche della soluzione, dimensionamento e soluzioni di scalabilità;
- Scelte progettuali e relative configurazioni il software di PKI per i servizi SPKI e il software per la gestione dei dati territoriali per RNDT;

c) Servizi di Governance:

- Descrizione di dettaglio dell'infrastruttura di elaborazione, architettura prescelta, caratteristiche tecniche della soluzione, dimensionamento e soluzioni di scalabilità;

d) Servizi di supporto all'Operatività:

- I CV delle figure professionali prescelte per i ruoli di Direttore Tecnico IC-SPC e Responsabile Operativo della Sicurezza;
- La struttura organizzativa prescelta per l'espletamento dei servizi, con particolare riferimento alle strutture di supporto (NOC, SOC, AOC e SEDE) e relative procedure di escalation.

3. **Specifiche di collaudo:** contenente le modalità di esecuzione dei test di collaudo, descritte tramite schede tecniche di dettaglio;
4. **Piano della Qualità:** contenente la descrizione dettagliata degli obiettivi di qualità relativi al servizio erogato e la descrizione sintetica dei processi di controllo della qualità (secondo quanto specificato nella Deliberazione CNIPA n. 49/2000 del 9 novembre 2000).
5. **Piano di Migrazione:** contenente il dettaglio della procedura di migrazione dei servizi attualmente erogati alla nuova infrastruttura oggetto della presente gara, comprensivo delle tempistiche di migrazione e delle modalità di roll-back.

[R.333] Il Progetto Esecutivo deve inoltre contenere le:

- **Regole di Interconnessione QXN** di cui al requisito [R.22]
- **Regole di interconnessione per l'adesione ai Servizi di Governance** contenente le modalità, gli obblighi, le regole e le specifiche di interconnessione a cui devono attenersi i soggetti che aderiscono ai Servizi di Governance.

[R.334] I **Piani di attivazione** di cui al punto 1) del requisito [R.332] e relativi ai soli servizi IQXN, SPKI, IPA e IGPEC devono prevedere una data di "pronto al collaudo" non superiore a 90 giorni solari rispetto alla data di approvazione del Progetto Esecutivo.

- [R.335] I **Piani di attivazione** di cui al punto 1) del requisito [R.332] e relativi ai soli servizi SGAC, SGQS, SGES, SGAW devono prevedere una data di “pronto al collaudo” non superiore a 180 giorni solari rispetto alla data di approvazione del Progetto Esecutivo.
- [R.336] I **Piani di attivazione** di cui al punto 1) del requisito [R.332] e relativi al servizio RNDT devono prevedere una data di “pronto al collaudo” non superiore a 240 giorni solari rispetto alla data di approvazione del Progetto Esecutivo.
- [R.337] I **Piani di attivazione** di cui al punto 1) del requisito [R.332] e relativi alle strutture e agli strumenti di cui ai paragrafi 4.3 e 4.4 devono prevedere la medesima data di “pronto al collaudo” dei servizi di cui rappresentano il supporto.

5.2 Collaudo

- [R.338] Il Fornitore, dopo aver completato le attività previste nei Piani di Attivazione , dovrà inviare ad AgID, a mezzo PEC, comunicazione di “Pronto al Collaudo”, fornendo evidenza di aver verificato la completa conformità di tutte le funzionalità tecnico/applicative sia ai requisiti esposti nel presente Capitolato Tecnico, sia a quelli esposti nei Progetti presentati nella Relazione Tecnica, sia a quelli riferibili ad eventuali caratteristiche aggiuntive contenute nel Progetto Esecutivo. La data di “Pronto al collaudo”, coincidente con la data di invio della predetta comunicazione via PEC, deve essere conforme a quanto previsto nei requisiti [R.334], [R.335], [R.336], [R.337].
- [R.339] Nei termini e nelle modalità previste il Fornitore deve supportare la Commissione di cui al requisito [R.340] nell’effettuazione delle necessarie prove di collaudo sia dei requisiti esposti nel presente Capitolato Tecnico, sia di quelli esposti nell’offerta tecnica presentata in gara, sia a quelli riferibili ad eventuali caratteristiche aggiuntive contenute nel Progetto Esecutivo o nella documentazione di riscontro.
- [R.340] Le attività di collaudo sono effettuate da un’apposita Commissione nominata da AgID, che esegue le prove previste dal Fornitore nelle “**Specifiche di collaudo**” di cui al punto 3) del requisito [R.332] ed ogni altra ulteriore prova che la stessa Commissione ritiene opportuna.
- [R.341] A conclusione delle attività della Commissione, la stessa redige un Verbale di Collaudo che riporta l’esito di tutte le prove effettuate.
- [R.342] Le attività di collaudo possono essere effettuate anche in modo parziale, relative a singole funzionalità o, comunque, ad una parte limitata dello specifico servizio.

- [R.343] Qualora AgID ed il Fornitore espressamente concordino nell'avviare l'erogazione dei servizi prima della conclusione con esito positivo delle attività di collaudo, il Fornitore applicherà ai servizi erogati prezzi unitari ridotti del 20% (ventipercento) rispetto ai corrispettivi contrattualmente previsti. La suddetta riduzione del 20% non sarà più applicata dalla data di superamento con esito positivo del collaudo. Per il periodo precedente alla suddetta data, non sarà effettuato alcun conguaglio e l'Amministrazione non riconoscerà ulteriori oneri oltre quelli già sostenuti.
- [R.344] A valle del buon esito del collaudo di ciascuno dei servizi IC-SPC, Il Fornitore concorda con l'Agenzia per l'Italia Digitale la messa in esercizio dei servizi nell'ambiente operativo predisposto.

5.3 Documentazione di riscontro

- [R.345] Il Fornitore deve aggiornare in corso d'opera (e, comunque, ad ogni cambiamento dei sistemi utilizzati) le specifiche esecutive di cui al punto 2 del [R.332] che costituiranno la documentazione di riscontro di seguito descritta. Tale documentazione dovrà essere resa disponibile ad AgID in formato elettronico (almeno in formato .pdf); è facoltà della stessa richiedere l'invio anche in formato cartaceo.
- [R.346] Il Fornitore deve predisporre la **documentazione di riscontro in conformità alla norma ISO 9004/2-91**, in particolare deve contenere almeno:
- **Le specifiche del servizio:** comprendenti una chiara descrizione delle caratteristiche del servizio (soggette a valutazione di AgID) e le condizioni di accettabilità per ciascuna caratteristica del servizio;
 - **Le specifiche di realizzazione del servizio:** comprendenti una 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.

- [R.347] Il Fornitore deve predisporre un **documento** denominato **Indice di Configurazione** in cui sia riportato e costantemente aggiornato l'elenco delle componenti HW e SW utilizzati per l'erogazione dei servizi previsti dal presente contratto.
- [R.348] Il Fornitore è tenuto a redigere e mantenere aggiornato il "**Documento di Organizzazione Tecnica**" che illustrerà in dettaglio le unità funzionali ed organizzative adottate all'interno delle strutture di cui al [R.267] ed i rapporti intercorrenti fra di esse e le strutture di supporto di cui al [R.260].
- [R.349] Il Fornitore deve predisporre un **Piano di Comunicazione** che soddisfi l'esigenza di identificare tutte le informazioni che ruotano intorno all'attività di esecuzione contrattuale al fine di assicurarne la completa diffusione a tutte le entità coinvolte e la gestione tempestiva di problemi attraverso una escalation di riferimento. Il Piano deve essere organizzato in linee di Servizio per ognuna delle quali si identificano le informazioni di seguito riportate:
- L'argomento della comunicazione;
 - La necessità di un atto formale a evidenza della comunicazione;
 - L'obiettivo della comunicazione;
 - Le responsabilità coinvolte per quella comunicazione;
 - La necessità di una lista di distribuzione (se diversa dai nomi presenti nella colonna responsabilità);
 - La modalità di comunicazione (es.: riunioni, conference call, e-mail);
 - La frequenza con cui la comunicazione deve essere svolta;
 - Lo standard da applicare alla comunicazione.
- [R.350] Il Fornitore deve predisporre il **Piano della Sicurezza** comprensivo dell'analisi del rischio, della sicurezza fisica, logica e organizzativa, disaster recovery e continuità operativa, prevenzione e gestione incidenti, allineamento continuo a norme, leggi, standard e best practice. Il **Piano della Sicurezza** deve rispondere ai requisiti previsti dalla norma ISO/IEC 27001:2005 per l'implementazione, il monitoraggio ed il miglioramento del Sistema di Gestione per la Sicurezza delle Informazioni (ISMS). Il Piano della Sicurezza sarà soggetto ad approvazione da parte di AgID.
- [R.351] Per tutte le attività che richiedono lo sviluppo di software, sia in caso di realizzazione che di manutenzione evolutiva, il Fornitore deve

produrre/aggiornare, in accordo e di concerto con AgID, un documento che descriva nel dettaglio le specifiche funzionali del software.

- [R.352] Il Fornitore, su richiesta di AgID, dovrà trasmettere all' AgID stessa entro il termine di 20 giorni solari, in apposito formato e su idoneo supporto informatico, la configurazione degli apparati e dei sistemi coinvolti nell'erogazione dei servizi oggetto del presente Capitolato.

6 Misurazione dei livelli di servizio e Reportistica

- [R.353] Il concorrente dovrà descrivere, nella Relazione Tecnica, le metodologie e le tecniche utilizzate per la misurazione dei parametri previsti nell'appendice "Livelli di Servizio e Penali".
- [R.354] Per la verifica del rispetto dei livelli di servizio contrattuali il Fornitore si impegna ad installare idonei strumenti di misura hardware e/o software e, ove non possibile, ad effettuare rilevazioni manuali dei parametri da misurare, secondo i requisiti richiesti nel presente Capitolato e quanto descritto nella Relazione Tecnica.
- [R.355] Su richiesta dei sottoscrittori dei contratti attuativi o di AgID, il Fornitore dovrà essere in grado di fornire idonea documentazione relativa ai malfunzionamenti (trouble ticket) verificatisi.
- [R.356] Tutti i dati rilevati alle misurazioni e tutti quelli oggetto dei report periodici dovranno essere archiviati e resi accessibili ad AgID e ai sottoscrittori dei contratti attuativi secondo quanto richiesto nel Capitolato e quanto descritto dal Fornitore nella Relazione Tecnica.
- [R.357] AgID si riserva la possibilità di richiedere ulteriori report periodici da concordare con il Fornitore.
- [R.358] La reportistica mensile di cui all'appendice "Livelli di Servizio e Penali" sarà prodotta dal Fornitore con riferimento al primo mese intero successivo alla data di avvio dei servizi.
- [R.359] AgID potrà richiedere in qualsiasi momento l'applicazione delle penali inerenti un report contrattuale, senza alcun limite temporale rispetto alla data di rilascio del report stesso.

Appendici:

- 1) SLA e Penali;
- 2) QXN;
- 3) SPKI;
- 4) RNDT;
- 5) IPA;
- 6) IGPEC;
- 7) Estratto della documentazione della procedura ristretta per l'affidamento dei servizi di connettività nell'ambito del Sistema Pubblico di Connettività.