

# RELAZIONE TECNICA

## Oggetto: interconnessione del SPC-Toscana con SPC-Centrale

### Premessa

Il presente documento è il risultato del gruppo di lavoro costituito da rappresentanti del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), della Regione Toscana e della Società Consortile QXN (SC-QXN) per lo studio di fattibilità di quanto in oggetto.

I partecipanti al gruppo di lavoro sono:

- CNIPA: Gaspare Ferraro, Vito Ammirata, Andrea Bartoli (Between), Gianluigi Moxedano
- Soc. Cons. QXN: Leonardo Gebbia, Mauro Mascagna
- Regione Toscana: Giovanni Armanino, Stefano Pimazzoni

I lavori del gruppo sono iniziati il 10/01/2007 e terminati con la redazione di questo documento il 05/04/2007.

### Il TIX

Il TIX è un'iniziativa della Rete Telematica Regione Toscana (RTRT) e svolge le funzioni di Neutral Access Point (NAP), cioè un punto d'interconnessione comune tra più Internet Service Provider (ISP) per lo scambio paritetico, cioè neutrale e senza privilegi, dei loro flussi IP attraverso lo stabilimento di canali diretti (peer) tra i domini di rete di ciascun ISP/peerer partecipante al NAP.

La partecipazione degli ISP al TIX avviene tramite la costituzione di un elenco di ISP accreditati, in grado di fornire servizi Internet alle pubbliche amministrazioni che desiderino aderire alla RTRT attraverso uno di tali provider. Attraverso il TIX la RTRT diventa quindi multifornitore.

### La QXN

La QXN è definita come la componente delle infrastrutture condivise in ambito SPC che realizza l'interconnessione delle reti dei fornitori dei servizi di connettività del SPC, delle reti territoriali e delle Community Network.

La componente QXN esistente è realizzata e gestita dalla Società Consortile QXN costituita dai quattro fornitori assegnatari della gara multifornitore bandita dal CNIPA ai sensi dell'art. 83 del dlgs. 7 marzo 2005 (Codice dell'Amministrazione Digitale).

Dal punto di vista tecnologico la Componente QXN esistente è stata progettata per realizzare l'interconnessione tra le reti afferenti alla stessa con un'affidabilità del 99,99%. E' pertanto costituita da due nodi ridondati, collegati tra loro con due link ad alta velocità su percorsi differenziati, collocati presso i maggiori NAP italiani: il MIX (NAP situato a Milano) ed il Namex (NAP situato a Roma).

I quattro fornitori assegnatari della gara multifornitore sono collegati ad entrambi i nodi con una configurazione ad alta affidabilità consistente nell'attestazione per ciascun nodo di una coppia di router, ognuno dei quali collegato ai due router della QXN che realizzano il singolo nodo.

## **Analisi del contesto**

Per la definizione degli aspetti progettuali connessi al collegamento in oggetto, è necessario innanzi tutto individuare i livelli di servizio che caratterizzano tale infrastruttura.

Da un'analisi svolta dai rappresentanti della Regione Toscana, basata su una stima dei fabbisogni di connettività della PAL toscana aderente alla RTRT verso SPC, emerge la necessità di prevedere i seguenti livelli di servizio minimi:

- Disponibilità unitaria: 99,9 %
- Tempo di ripristino del servizio:
  - disservizi di tipo "bloccante"
    - 4 h nel 95% dei casi
    - 8 h nel 100% dei casi
  - disservizi di tipo "non bloccante"
    - 8 h nel 95% dei casi
    - 16 h nel 100% dei casi
  - disservizi di tipo "anomalia"
    - 3 gg nel 100% dei casi
- Finestra temporale di erogazione:
  - per quanto riguarda la disponibilità
    - 00.00-24.00, 7 gg su 7
  - per quanto riguarda i tempi di ripristino
    - 08.00-20.00 feriali
    - 08.00-14.00 sabato
- OWD < 60 ms per il 95% dei pacchetti
  - considerando pacchetti di 200 bytes, trasmessi in numero di 10 pkt/min e 200 ms di intervallo di tempo tra due pacchetti successivi in condizioni di link non saturo.
- Packet Loss < 0,1%

Dalla medesima analisi emerge una stima di traffico aggregato verso la restante parte di SPC, basata sui dati relativi all'attuale collegamento della RTRT alla Rete Unitaria della Pubblica Amministrazione (RUPA) ed alla Rete Interregionale, di circa 10 Mbps.

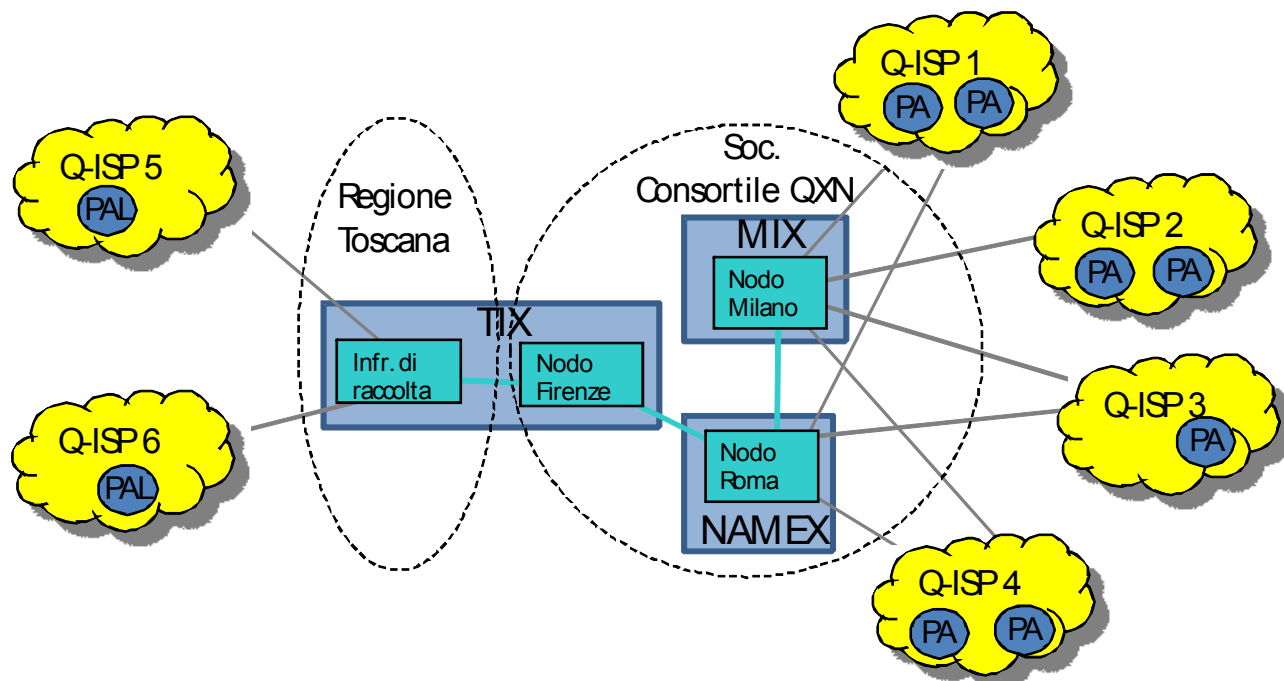
Il servizio dovrà essere attivo h24x365 giorni l'anno.

## **Soluzione proposta**

Il gruppo di lavoro, dopo aver analizzato varie soluzioni, e tenendo conto non soltanto degli obiettivi tecnici minimi ma anche delle esigenze di definizione dei limiti di responsabilità per la gestione dell'infrastruttura, individua la seguente soluzione:

- un collegamento geografico ridondato tra Firenze (sede del TIX) e uno degli attuali nodi del Componente QXN esistente, terminato su una coppia di router; tale infrastruttura sarà gestita dalla Soc. Cons. QXN;
- una infrastruttura presso il TIX per la raccolta del traffico SPC dei fornitori qualificati toscani; la gestione di tale infrastruttura sarà responsabilità della Regione Toscana.

La seguente figura riassume l'architettura proposta:



Per la realizzazione del collegamento geografico, in base ai parametri prestazionali e dimensionali precedentemente indicati, la Soc. Cons. QXN ritiene idoneo l'utilizzo di due link della capacità di 20 Mbps SDH collegati in doppia via al solo nodo di Roma, terminati presso il TIX su n. 2 Border Router (BR) della classe 7600 equipaggiati con alimentazione ridondata e porte di accesso gigabit ethernet miste rame / fibra.

Gli oneri necessari per la realizzazione e gestione di tale infrastruttura sono stimati dell'ordine di 150.000 € di investimenti e di 95.000 €/anno per i canoni di gestione e manutenzione.

Per la realizzazione dell'infrastruttura di raccolta presso il TIX, i rappresentanti della Regione Toscana ritengono idonea una soluzione progettuale che prevede l'installazione di n.2 Border Router (BR) della classe Cisco 6500, equipaggiati con alimentazione ridondata, doppia engine da 720 Gbps, porte di accesso gigabit ethernet miste rame / fibra.

Gli oneri necessari per la realizzazione e gestione di tale infrastruttura di raccolta sono stimati dell'ordine di 200.000 € di investimenti e di 30.000 €/anno per i canoni di manutenzione.

Tale coppia di router, appartenenti ad uno specifico AS pubblico dedicato, che svolga funzioni di transit verso l'AS della componente QXN esistente, dovrà quindi essere collegata alla sopracitata coppia di router in gestione alla Soc. Cons. QXN

Al fine di garantire il corretto funzionamento del routing in ambito SPC, le regole di peering tra l'infrastruttura di raccolta e gli AS dei fornitori qualificati toscani dovranno essere le stesse previste tra l'AS della QXN e gli AS dei fornitori qualificati nazionali, così come previsto dalle regole tecniche del SPC.

L'infrastruttura di raccolta farà quindi peering con l'AS della QXN e svolgerà le funzioni di AS di transito per i fornitori qualificati toscani verso/da tutti gli altri fornitori qualificati in ambito SPC.

L'infrastruttura di raccolta dovrà possedere le seguenti caratteristiche minime:

- essere coerente con le regole tecniche e di sicurezza definite in ambito SPC
- utilizzare un AS dedicato a svolgere esclusivamente funzioni di AS di transito;
- non ammettere il peering con soggetti diversi dalla QXN o dai fornitori qualificati toscani.

L'infrastruttura complessiva erogherà ai fornitori qualificati toscani il servizio di interconnessione alla QXN secondo i seguenti livelli di servizio minimi:

- Disponibilità unitaria: 99,9 %
- Tempo di ripristino del servizio:
  - disservizi di tipo "bloccante"
    - 4 h nel 95% dei casi
    - 8 h nel 100% dei casi
  - disservizi di tipo "non bloccante"
    - 8 h nel 95% dei casi
    - 16 h nel 100% dei casi
  - disservizi di tipo "anomalia"
    - 3 gg nel 100% dei casi
- Finestra temporale di erogazione:
  - per quanto riguarda la disponibilità
    - 00.00-24.00, 7 gg su 7
  - per quanto riguarda i tempi di ripristino
    - 08.00-20.00 feriali
    - 08.00-14.00 sabato

Il servizio sarà attivo h24x365 giorni l'anno.

L'infrastruttura di collegamento tra Firenze e Roma sarà gestita dal Network Operating Center (NOC) e dal Security Operation Center (SOC) della Soc. Cons. QXN.

L'infrastruttura di raccolta sarà gestita dal Network Operating Center (NOC) e dal Security Operation Center (SOC) della Regione Toscana.

## **DNS**

Per motivi di sicurezza, è al momento in fase di attuazione un servizio di DNS esclusivo

all'interno di SPC per la risoluzione di nomi Infranet, non pubblicabili su Internet. Tale servizio DNS della rete SPC è visto come un servizio federato di DNS. Gli attori fino ad ora coinvolti per l'erogazione del servizio sono gli operatori qualificati (QISP) e la società consortile QXN.

Rispetto a questo scenario, anche l'infrastruttura di raccolta della Regione Toscana ed i Q-ISP regionali ad essa afferenti debbono essere parte integrante del servizio.

Modello:

- **QISP regionale (QISPr):** fornisce un DNS (DNS QISPr) dedicato alle rispettive PAL ad esso afferenti. Il DNS del QISPr è slave dei DNS delle PAL afferenti o master nel caso queste ultime non abbiano un proprio DNS. Nel primo caso, mediante zone transfer, vengono replicate su di esso tutte le zone presenti nei DNS delle PAL afferenti. Pertanto, il DNS del QISPr è autorevole per tutti i nomi a dominio delle PAL afferenti.
- **Infrastruttura di raccolta presso TIX:** fornisce un DNS (DNS SPC-T) dedicato ai rispettivi QISPr afferenti. Il DNS SPC-T è slave dei DNS QISPr afferenti: mediante zone transfer vengono replicate su di esso tutte le zone presenti nei DNS QISPr afferenti. Pertanto, il DNS SPC-T è autorevole per tutti i nomi a dominio delle PAL afferenti ai QISPr connessi alla infrastruttura di raccolta presso TIX.
- Analogamente tale organizzazione è ovviamente la replica di quanto presente anche a livello di QISP e del DNS QXN.
- DNS QXN e DNS SPC-T conoscono tutti i domini delle PA SPC di rispettiva competenza.
- Al fine di avere almeno un punto dove tutte le informazioni sulle zone Infranet e Internet SPC siano note, per motivi di robustezza della soluzione, si conviene che DNS QXN sia configurato come slave di tutte le zone presenti su DNS SPC-T.

Tutti i DNS coinvolti dovranno effettuare il "forwarding" delle richieste relative alle zone per le quali non sono autorevoli, realizzando così una federazione di DNS interno al SPC.

Si prospettano due modalità di federare i vari DNS coinvolti:

- *forwarding* incondizionato (di tutte le zone Infranet e Internet) fino al DNS QXN
- *forwarding* selettivo (delle sole zone Infranet) fino al DNS QXN, stante la pubblicazione della lista dei domini Infranet (informazione già necessaria per la configurazione dei DNS slave)

Si rinvia a fasi tecniche specifiche successive la scelta e lo studio della soluzione da applicare.

E' necessario comunque che Regione Toscana si doti di una piattaforma HW/SW per l'implementazione del servizio DNS sopra indicato secondo le modalità tecniche che verranno concordate.

### **Conclusioni**

L'interconnessione del SPC-Toscana con SPC-Centrale è tecnicamente fattibile attraverso la realizzazione di una infrastruttura costituita da un collegamento tra il TIX e il nodo QNX di Roma e da un'infrastruttura di raccolta che si interfaccia da un lato con i fornitori qualificati toscani e dall'altro con tale collegamento.

Il gruppo di lavoro ha anche svolto un'analisi di dettaglio relativamente agli aspetti connessi ai piani di indirizzamento e alle politiche di routing che ha permesso di verificare, dal punto di vista teorico, il corretto funzionamento della soluzione architetture individuata.

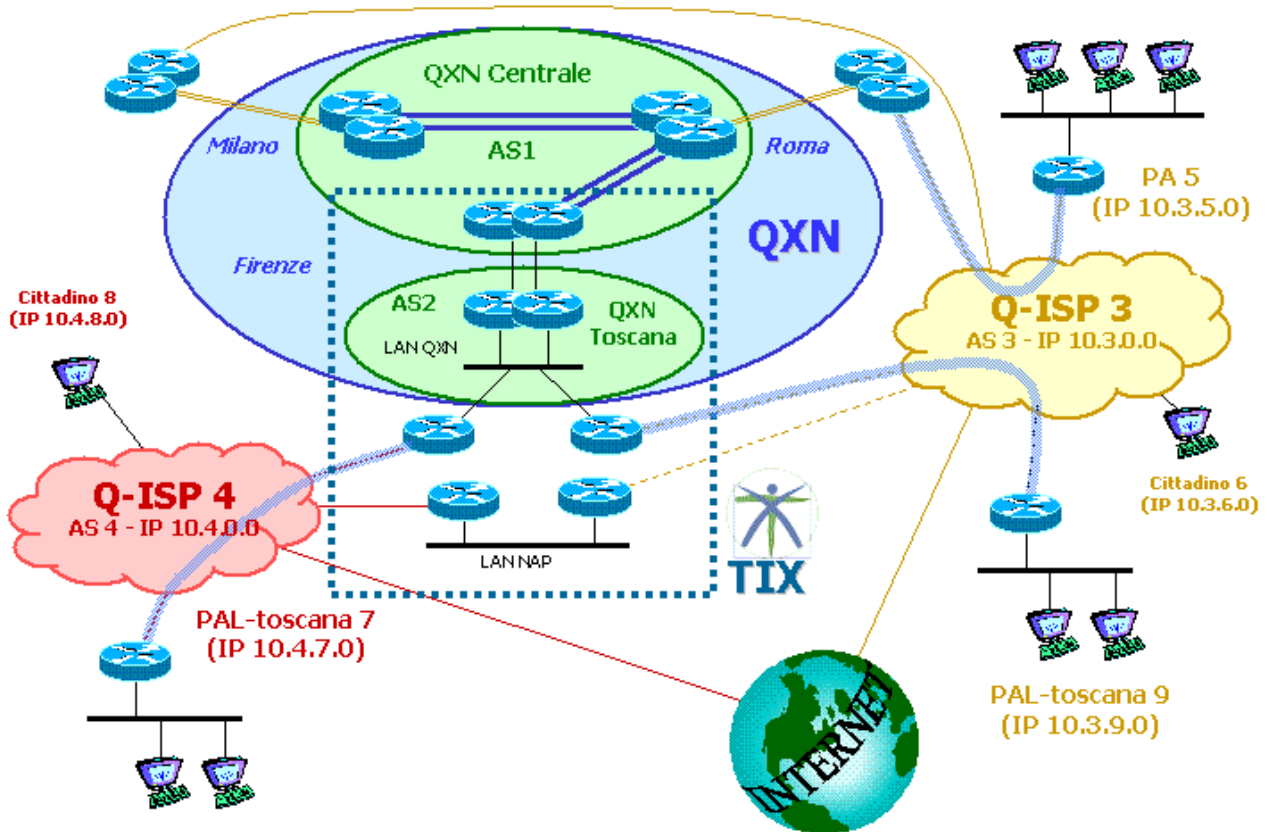
Si ritiene comunque necessario, qualora le soluzioni tecniche sopra individuate venissero adottate, una progettazione di dettaglio che definisca sia gli apparati che le configurazioni degli stessi.

Dal punto di vista organizzativo si segnala infine la necessità di definire opportunamente i rapporti contrattuali tra tutti i vari attori, al fine di garantire l'erogazione dei servizi in un contesto nel quale siano puntualmente definiti i vari confini di responsabilità.

## ALLEGATO A

### Analisi dei flussi di traffico

L'infrastruttura ipotizzata risulta pertanto quella rappresentata nella figura seguente, dove sono stati evidenziati, oltre all'infrastruttura QXN, anche un Q-ISP "centrale" ed un Q-ISP "toscano" con i relativi Border Router; i percorsi semitrasparenti che collegano i router delle PA ai relativi BR-QXN evidenziano le tecniche di segregazione del traffico.



Al fine di valutare i possibili flussi di traffico, si fanno le seguenti ipotesi:

- la componente QXN esistente ha l'AS1 e la QXN-toscana l'AS2;
- il Q-ISP 3 ha l'AS 3 e la classe 10.3.0.0/16 di indirizzi IP, di cui la 10.3.5.0/24 assegnata alla PAC5, la 10.3.9.0/24 alla PAL-toscana9 e la 10.3.6.0/24 al Cittadino/Impresa6
- il Q-ISP 4 ha l'AS4 e la classe IP 10.4.0.0/16, di cui la 10.4.7.0/24 assegnata alla PAL-toscana7 e la 10.4.8.0/24 al Cittadino/Impresa8

In queste ipotesi,

il Q-ISP3 annuncia le seguenti reti:

- 10.3.0.0/16 su Internet e sui NAP pubblici a cui è attestato
- 10.3.5.0/24 sul QXN con entrata preferenziale Roma (o Milano)
- 10.3.9.0/24 sul QXN con entrata preferenziale Firenze

mentre il Q-ISP4 annuncia:

- 10.4.0.0/16 su Internet e sul TIX

- 10.4.7.0/24 sul QXN a Firenze

Sul QXN vengono viste le seguenti reti:

- 10.3.5.0/24 del Q-ISP3 con uscita preferenziale Roma (o Milano)
- 10.3.9.0/24 del Q-ISP3 con uscita preferenziale Firenze
- 10.4.7.0/24 del Q-ISP4 con uscita a Firenze

mentre su Internet troviamo le reti:

- 10.3.0.0/16 annunciata dal Q-ISP3
- 10.4.0.0/16 annunciata dal Q-ISP4

Di conseguenza la matrice di traffico risulta la seguente:

da \ a	PAC5	Citt/Impr6	PAL7	Citt/Impr8	PAL9
<b>PAC5</b>	-	AS3	AS3-AS1- AS2-AS4	AS3-Internet- AS4	AS3
<b>Citt/Impr6</b>	AS3	-	AS3-Internet- AS4	AS3-Internet- AS4	AS3
<b>PAL7</b>	AS4-AS2- AS1-AS3	AS4-Internet- AS3	-	AS4	AS4-AS2- AS3
<b>Citt/Impr8</b>	AS4-Internet- AS3	AS4-Internet- AS3	AS4	-	AS4- Internet-AS3
<b>PAL9</b>	AS3	AS3	AS3-AS2-AS4	AS3-Internet- AS4	-