REPUBBLICA ITALIANA

BOLLETTINO UFFICIALE

DELLA REGIONE PUGLIA

Sped. in abb. Postale, Art. 2, comma 20/c - Legge 662/96 - Aut. DC/215/03/01/01 - Potenza

Anno XXXIII | BARI, 17 SETTEMBRE 2002 | N. 117

Il Bollettino Ufficiale della Regione Puglia si pubblica con frequenza infrasettimanale ed è diviso in due parti.
Nella 1ª parte si pubblicano: Leggi e Regolamenti regionali, Ordinanze e sentenze della Corte Costituzionale e di Organi giurisdizionali, Circolari aventi rilevanza esterna, Deliberazioni del Consiglio regionale riguardanti l'elezione dei componenti l'Ufficio di presidenza dell'Assemblea, della Giunta e delle Commissioni permanenti.
Nella 2ª parte si pubblicano: le deliberazioni del Consiglio regionale e della Giunta; i Decreti del Presidente, degli Assessori, dei funzionari delegati, di pubbliche autorità; gli avvisi, i bandi di concorso e le gare di appalto.
Gli annunci, gli avvisi, i bandi di concorso, le gare di appalto, sono inseriti nel Bollettino Ufficiale pubblicato il giovedì.
Direzione e Redazione - Presidenza Giunta Regionale - Lungomare N. Sauro, 33 - 70121 Bari - Tel. 0805406316-0805406317-0805406372 - Uff. abbonamenti 0805406376 - Fax 0805406379.
Abbonamento annuo di € 134,28 tramite versamento su **c.c.p. n. 18785709 intestato a Regione Puglia - Ufficio Bollettino Ufficiale - Lungomare N. Sauro, 33 - Bari.**
Prezzo di vendita € 1,34. I versamenti per l'abbonamento effettuati entro il 15° giorno di ogni mese avranno validità dal 1° giorno del mese successivo; mentre i versamenti effettuati dopo il 15° giorno e comunque entro il 30° giorno di ogni mese avranno validità dal 15° giorno del mese successivo.

Gli annunci da pubblicare devono essere inviati almeno 3 giorni prima della scadenza del termine utile per la pubblicazione alla Direzione del Bollettino Ufficiale - Lungomare N. Sauro, 33 - Bari.
Il testo originale su carta da bollo da € 10,33, salvo esenzioni di legge, deve essere corredato da 1 copia in carta uso bollo e dall'attestazione del versamento della tassa di pubblicazione prevista.
L'importo della tassa di pubblicazione è di € 154,94 oltre IVA al 20% (importo totale € 185,93) per ogni inserzione il cui contenuto non sia superiore, nel testo, a quattro cartelle dattiloscritte pari a 100 righe per 60 battute (o frazione) e di € 11,36 oltre IVA (importo totale € 13,63) per ogni ulteriore cartella dattiloscritta di 25 righi per 60 battute (o frazione).
Il versamento dello stesso deve essere effettuato sul c.c.p. n. 18785709 intestato a **Regione Puglia - Ufficio Bollettino Ufficiale Bari.**
Non si darà corso alle inserzioni prive della predetta documentazione.
LE PUBBLICAZIONI SONO IN VENDITA PRESSO LA LIBRERIA UNIVERSITÀ E PROFESSIONI SRL - VIA CRISANZIO 16 - BARI; LIBRERIA PIAZZO - PIAZZA VITTORIA, 4 - BRINDISI; CASA DEL LIBRO - VIA LIGURIA, 82 - TARANTO; LIBRERIA PATIERNO ANTONIO - VIA DANTE, 21 - FOGGIA; LIBRERIA MILELLA - VIA PALMIERI 30 - LECCE.

SOMMARIO

PARTE SECONDA

Deliberazioni del Consiglio regionale e della Giunta

PARTE SECONDA

Deliberazioni del Consiglio regionale e della Giunta

DELIBERAZIONE DELLA GIUNTA REGIONALE 8 agosto 2002, n. 1092

POR Puglia 2000-2006 Misura 6.3 – azione a) "Creazione dell'infrastruttura telematica di base della RUPA regionale". Approvazione Progetti e capitolati tecnici.

Il Presidente della Giunta, sulla base dell'istruttoria espletata dal Dirigente Responsabile del Settore Segreteria della Giunta di concerto con il Dirigente Responsabile dell'Area delle Politiche Comunitarie, riferisce quanto segue.

PREMESSO:

- *che la Regione Puglia con legge regionale n. 13 del 25 settembre 2000 ha regolamentato le "Procedure per l'attivazione del Programma Operativo della Regione Puglia 2000-2006";*

- che con deliberazione della Giunta Regionale n.1255 adottata nella seduta del 10 ottobre 2000 è stato approvato il Programma Operativo Regionale (POR) Puglia 2000-2006;

- che nella citata deliberazione n.1255/2000 all'Asse VI "Rafforzamento delle Reti e dei nodi di servizio" è prevista la Misura 6.3 "Sostegno all'innovazione degli Enti Locali" che si pone quale obiettivo specifico di *sostenere e diffondere la Società dell'Informazione con particolare riferimento ai settori della Pubblica Amministrazione, dell'educazione pubblica e dei sistemi produttivi;*

- che la Azione a) della Misura 6.3 prevede la "Creazione dell'infrastruttura telematica di base della RUPA regionale" che prevede la realizzazione dei seguenti obiettivi come specificati dal Complemento di Programmazione (CdP): *«L'intervento ha come obiettivo la realizzazione, gestione ed evoluzione di una infrastruttura telematica di base che garantisca: la connettività di livello geografico tra le varie sedi delle amministrazioni pubbliche regionali (Regione, Province, Comuni) mediante l'uso di circuiti trasmissivi sia fisici che virtuali, comprendendo in questi ultimi anche infrastrutture di reti private virtuali su protocollo IP; l'integrazione tecnico-funzionale con la Rete Unitaria della Pubblica Amministrazione, anche attraverso gli specifici protocolli di interconnessione da questa definiti; l'espletamento in modo puntuale dell'attività di monitoraggio di ogni circuito, della registrazione dei volumi di traffico, dell'emissione degli addebiti alle singole amministrazioni e della pronta individuazione delle anomalie nei circuiti forniti alle reti senza che queste debbano necessariamente essere denunciate dall'utenza; la disponibilità di servizi di interconnessione e di interoperabilità a livello applicativo tra le Amministrazioni e con l'esterno, quali in particolare: posta elettronica; trasferimento di file; terminale virtuale; accesso a News; accesso a World Wide Web. La Rupa regionale dovrà essere realizzata in coerenza con le raccomandazioni sul fronte tecnico e applicativo dell'AIPA e con le politiche e i piani nazionali in materia di sviluppo dei servizi on-line della Pubblica Amministrazione (cosiddetto e-government). Essa dovrà inoltre agevolare l'integrazione delle reti settoriali, di categoria e di area territoriale già operative in sede locale»;*

- che la Giunta regionale con propria deliberazione n.1162 del 10 agosto 2001 ha approvato la Convenzione con la Società Tecnopolis;

- che l'art. 2 della citata Convenzione stabilisce che alla Società Tecnopolis compete la realizzazione del progetto preliminare e dei relativi capitolati per la realizzazione della RUPA regionale di cui alla Azione a) della Misura 6.3;

- che alla realizzazione del progetto e capitolati la Società Tecnopolis deve provvedere mediante il Centro Tecnico da costituirsi secondo le modalità indicate all'art. 3 della Convenzione;

- che la Giunta con delibera n. 227 del 19/03/2002 ha preso atto della costituzione del Centro Tecnico e dell'effettivo inizio delle attività;

- che il Progetto strategico deve essere redatto in coerenza con le raccomandazioni sul fronte tec-

nico e applicativo indicate dal Centro Tecnico nazionale ex AIPA sentite le esigenze delle principali amministrazioni ed enti regionali di cui è prevista la connessione;

RILEVATO che in data 16/07/2002 il Presidente della Giunta, a seguito di convocazione (prot. n.1870/FC del 10/07/2002), ha tenuto specifica riunione con i Presidenti delle Delegazioni regionali dell'ANCI, UPI ed UNCEM nella quale è stato presentato il progetto strategico;

RILEVATO che il data 23/07/2002 con nota n. 953/1D116 il Centro Tecnico ha trasmesso i capitolati tecnici aggiornati sulla base degli incontri con il Centro Tecnico della rete nazionale (29/01/2002) e con le Autonomie Locali regionali (16/07/2002);

Si propone, pertanto, alla Giunta di approvare il Piano Strategico di sviluppo della RUPAR, del Progetto Tecnologico del Centro tecnico ed i relativi capitolati tecnici per la "Creazione dell'infrastruttura telematica di base della RUPA regionale " di cui alla Misura 6.3 azione a) predisposti dal Centro Tecnico di Tecnopolis a norma della Convenzione e delle indicazioni di cui alla DGR n.1162/2001.

ADEMPIMENTI CONTABILI DI CUI ALLA L.R. N. 28/2001 E S.M.

Il presente atto non comporta adempimenti contabili di cui alla L.R. n.28/2002 e s.m.

Per i successivi adempimenti contabili si farà riferimento ai capitoli di spesa previsti per i cofinanziamenti del FESR per la Misura 6.3 "1091603 (quota UE-Stato)" e "1095603 (quota Regione)".

Il Presidente relatore, sulla base delle risultanze istruttorie come innanzi illustrate propone alla Giunta l'adozione del conseguente atto finale.

Il presente atto rientra nelle competenze della Giunta regionale ai sensi dell'art 4, comma 4, lettera a) e d) della L.R. n.7/1997 e dell'art. 2 comma 7 della Convenzione stipulata con la Società Tecnopolis.

LA GIUNTA

Udita la relazione del Presidente della Giunta;

Vista la sottoscrizione posta in calce al presente provvedimento dal Dirigenti Responsabili del Settore Segreteria della Giunta e dell'Area delle Politiche Comunitarie;

A voti unanimi espressi nei modi di legge,

DELIBERA

- di approvare il Piano strategico di sviluppo, il Progetto del Centro Erogazione Servizi ed i relativi capitolati tecnici per la "Creazione dell'infrastruttura telematica di base della RUPA regionale " di cui alla Misura 6.3 azione a) redatti dal Centro Tecnico di Tecnopolis secondo le indicazioni di cui alla DGR n.1162/2001 allegati al presente provvedimento del quale formano parte integrante:
  - Allegato "A" Piano Strategico di Sviluppo;
  - Allegato "B" Progetto del Centro di Erogazione Servizi Tecnologici del Centro Tecnico;
  - Allegato "C" Capitolato Tecnico del Servizio di Trasporto ed Interoperabilità di base;
  - Allegato "D" Capitolato Tecnico del Servizio di Firma Digitale;
  - Allegato "E" Capitolato Tecnico del Servizio di locazione dei nodi (EPO-LP) della RUPAR;
  - Allegato "F" Modulo di adesione delle Amministrazioni Locali alla RUPAR;

- di stabilire che alla dotazione delle apparecchiature del Progetto del Centro di Erogazione Servizi Tecnologici del Centro Tecnico di cui all'Allegato "B", si provvederà secondo le modalità e procedure definite nel manuale di rendicontazione delle spese ammissibili (lettera G) approvato con DGR n.227/2002;

- di incaricare il competente Settore AA.GG. – Ufficio Contratti ed Appalti alla pubblicità ed all'espletamento delle procedure di gara secondo la vigente normativa comunitaria, nazionale e regionale in materia;

- di disporre la pubblicazione del presente provvedimento e dei relativi allegati sul BURP.

Il Segretario
Dott. Romano Donno

Il Presidente
On. dott. Raffaele Fitto

Tecnopolis CSATA

Regione Puglia

Rete Unitaria della Pubblica Amministrazione Regionale

(R.U.P.A.R)

Piano Strategico di Sviluppo

(prodotto nell'ambito della Convenzione approvata dalla Giunta Regionale con deliberazione n. 1162 del 10/8/2001)

Allegato A

Versione 2.0 del 30 aprile 2002

INDICE DEGLI ARGOMENTI

Nomenclatura e acronimi

RN	Rete Nazionale
VPN	Virtual Private Network (Rete Virtuale Privata)
PdR	Porta di Rete
RUPA	Rete Unitaria della Pubblica Amministrazione (Centrale)
RUPAR	Rete Unitaria della Pubblica Amministrazione Regionale
FSR	Fornitore Servizi RUPAR (Trasporto ed Interoperabilità)
FSFD	Fornitore Servizi Firma Digitale
FSA	Fornitore Servizi Applicativi
CT	Centro Tecnico

Premessa

Nel Programma Operativo Regionale 2000/2006, la Regione Puglia ha deciso (Misura 6.3, Sottomisura A, Azione a) di realizzare la Rete Unitaria della Pubblica Amministrazione Regionale (RUPAR Puglia), e ne ha affidato, con Delibera della Giunta Regionale n. 1162 del 10/8/2001, la progettazione a Tecnopolis CSATA.

Tecnopolis ha redatto il presente progetto, la cui impostazione è stata oggetto di ampio e positivo confronto con il Centro Tecnico della Rete Nazionale e con esperti del settore.

A Il profilo strategico, l'impianto e la gestione della RUPAR

A.1 Introduzione

Nel presente documento la **RUPAR** (**R**ete **U**nitaria della **P**ubblica **A**mministrazione **R**egionale) **della Regione Puglia** è descritta facendo il più possibile uso, ove appropriato, della stesse terminologie adottate prima dall'AIPA per la descrizione della RUPA e poi dal Centro Tecnico della **R**ete **N**azionale per la descrizione della omonima rete.

Questa scelta è opportuna dato che la RUPAR si ispira ai due modelli e sarà interconnessa alle due reti con il compito di servire con capillarità le Pubbliche Amministrazioni Locali (PAL) della Regione Puglia. L'adozione di una medesima terminologia facilita la comprensione per chi ha già dimestichezza con la problematica a livello nazionale o in altre regioni ed inoltre facilita la mappatura dei servizi offerti dalla RUPAR-Puglia rispetto a quelli disponibili in altri contesti.

Oltre alle PAL propriamente dette (Regione, Province, Comuni) la rete deve poter gestire l'interconnessione anche di altri soggetti operanti all'interno del sistema dei pubblici servizi o a loro correlati da specifiche funzioni (p. es. ASL, Comunità Montane etc. etc.): la generica Entità che usufruisce dei servizi RUPAR sarà nel seguito definita Amministrazione.

Questo documento ha lo scopo di presentare azioni, tempi, risorse e costi per la realizzazione ed il funzionamento della Rete Unitaria della Pubblica Amministrazione Regionale della Puglia (RUPAR Puglia).

La RUPAR Puglia realizza il collegamento telematico delle amministrazioni locali della Puglia e tramite la Rete Nazionale collega gli enti pugliesi alle altre comunità di Pubbliche Amministrazioni italiane.

A.1.1 Il quadro di riferimento

La realizzazione della RUPAR Puglia è prevista dalla **Misura 6.3**, "**Sostegno all'innovazione degli Enti Locali**", del POR Puglia 2001-2006 che rappresenta, al momento, il principale strumento di attuazione delle politiche del Governo regionale.

La Misura 6.3 ha come obiettivo lo sviluppo e la diffusione della Società dell'Informazione in Puglia con particolare riferimento ai settori della Pubblica Amministrazione, dell'educazione pubblica, e dei sistemi produttivi. Responsabile della Misura è la Presidenza della Giunta della Regione Puglia a sottolineare la rilevanza che questo obiettivo riveste per il governo regionale. I destinatari degli interventi sono le Amministrazioni Pubbliche della Puglia.

Lo sviluppo e la diffusione della Società dell'Informazione in Puglia sono perseguiti in modo organico dalla Regione anche da altre due Misure del POR, la **Misura 6.2** ("Società dell'Informazione") e la **Misura 6.4** ("Risorse Umane e Società dell'Informazione"), oltre che, in modo più distribuito, da quasi tutte le

altre Misure a testimonianza della trasversalità della Società dell'Informazione rispetto a tutti gli aspetti della vita sociale ed economica.

La Misura 6.2, "**Società dell'Informazione**", ha come obiettivi specifici il Piano regionale per la Società dell'Informazione, il sostegno all'internazionalizzazione delle imprese pugliesi e la promozione dell'integrazione economica transfrontaliera e transnazionale.

La Misura 6.4, "**Risorse Umane e Società dell'Informazione**", punta invece allo sviluppo ed alla diffusione delle conoscenze e dei contenuti applicativi connessi con l'applicazione delle tecnologie dell'informazione, della comunicazione e delle reti infotelematiche, con particolare riferimento alla costruzione ed implementazione della Rete della PA (RUPA e RN).

La Misura 6.3 si articola su due linee di interventi: la prima ha come obiettivo la realizzazione della RUPAR Puglia; la seconda l'adeguamento strutturale ed operativo dei centri dei servizi per l'impiego nell'ambito della società dell'informazione ed è strettamente coordinata con gli interventi previsti nella Misura 3.1, "Organizzazione del sistema dei servizi per l'impiego".

Ritornando più specificamente alla RUPAR, essa comunicherà con altre comunità di PA, ivi compresa, la RUPA (Rete Unitaria della Pubblica Amministrazione).

Il progetto della RUPA è, di fatto, l'iniziativa più importante dell'Autorità per l'Informatica nella PA (AIPA) che, ai sensi del D.lg. 39/93, ha compiti di indirizzo, pianificazione e controllo della informatizzazione del settore pubblico.

Con la RUPA l'AIPA ha inteso determinare le condizioni infrastrutturali per la realizzazione del Sistema Informativo Unitario della Pubblica Amministrazione. Sistema Informativo che, nelle intenzioni dell'AIPA, dovrebbe consentire alla Pubblica Amministrazione di recuperare efficienza, efficacia e unitarietà di funzionamento rispettando e, auspicabilmente elevando, autonomia e responsabilità dei singoli enti. L'adesione alla RUPA è obbligatoria per le sole amministrazioni centrali.

Nel progetto RUPA gli Enti Locali, anche se non obbligati ad aderire, svolgono un ruolo fondamentale come fornitori di informazioni e servizi necessari per i sistemi informatici delle amministrazioni centrali, come attori di processi di cooperazione che coinvolgono i sistemi informatici delle amministrazioni centrali e locali e, soprattutto, come erogatori di servizi finali verso i cittadini.
Possono aderire alla RUPA o singolarmente o in associazione dopo aver costituito una RUPA locale. Le RUPA locali costituite dalle Regioni sono denominate RUPAR.

RUPAR regionali sono state promosse, oltre che dalla Regione Puglia, anche da altre Regioni tra cui la Toscana, il Piemonte, la Lombardia, l'Emilia Romagna e la Basilicata.

Nel giugno 2000 il progetto RUPA è stato in gran parte ripreso, integrato e finanziato dal Piano di Azione per l'e_Government messo a punto dalla Funzione Pubblica. Il Piano di e_Government inserisce la RUPA nella **Rete Nazionale** delle Amministrazioni (**RN**).

La **RN**, infatti, amplia i confini della RUPA, estendendosi a tutti i livelli della PA, alle reti di categoria ed ai centri di servizi. Dal punto di vista tecnico non prevede la costituzione di una nuova infrastruttura telematica ma punta a qualificare la Internet italiana, lasciando a ciascuna amministrazione la scelta di acquisire i servizi di rete da uno dei tanti Internet Service Provider che operano sul libero mercato con la sola condizione di adottare i criteri stabiliti dal Centro Tecnico della RN.

Dal punto di vista architetturale la Rete Nazionale si configura come una rete che connette:

- la RUPA stessa;
- le RUPA regionali (RUPAR);
- le reti promosse da Province, Comunità montane, Città Metropolitane e Comuni;

- le cosiddette **Community Network** (CN), ovvero le reti di categoria.

Il Piano di Azione per l'e_Government affronta esclusivamente gli aspetti della Società dell'Informazione che si riferiscono all'utilizzo dell'*Information Communication Technologies* (ICT) nelle attività delle Pubbliche Amministrazioni.

Le ipotesi di sviluppo della Società dell'Informazione in Italia sono invece affrontate in modo ampio dal Forum per la Società dell'informazione, organismo istituito dalla Presidenza del Consiglio dei Ministri. Nell'estate del 2000, il Forum ha prodotto, con il contributo di numerosi studiosi ed organizzazioni, il Rapporto sullo Sviluppo della Società dell'Informazione.

Il Rapporto propone obiettivi e priorità raggiungibili attraverso il lavoro congiunto di una pluralità di attori tra cui le stesse istituzioni pubbliche, le imprese, le organizzazioni sindacali, il sistema bancario, il mondo della finanza e dei servizi, il settore educativo e della ricerca, le associazioni del volontariato.

Il fine ultimo è la costruzione di una società più giusta e più ricca, in grado di valorizzare meccanismi decisionali reticolari e condivisi e di promuovere i fenomeni di innovazione e rinnovamento, nonché la capacità di rimettere tutto continuamente in discussione.

Il Piano di Azione per l'e_Government ed il Rapporto sullo Sviluppo della Società dell'Informazione si rifanno direttamente all'iniziativa "***eEurope – Una società dell'informazione per tutti***", lanciata l'8 dicembre 1999 dalla Commissione europea.

Durante il Consiglio europeo straordinario di Lisbona del 23-24 marzo 2000 l'Italia ha ottenuto che nelle conclusioni fosse posta in risalto la necessità che l'azione comunitaria sia rivolta soprattutto alla valorizzazione delle attività che si svolgono nel territorio, tenendo conto in particolare del fatto che le aree più disagiate richiedono interventi specifici. Inoltre nel documento si è indicato il ruolo importante che gli enti territoriali sono chiamati a svolgere per lo sviluppo della società dell'informazione.

Il 16 Giugno 2000 il Comitato dei Ministri per la Società dell'informazione ha varato il Piano di Azione per la Società dell'informazione che è stato diviso in quattro aree: capitale umano; e-government; e-commerce; infrastrutture, concorrenza e accesso. Il Piano di Azione rappresenta un integrazione del Piano di Azione eEurope 2002 approvato il 19-20 giugno 2000 dal Consiglio europeo.

Il POR Puglia tiene conto delle indicazioni contenute nel Piano eEurope, nel Piano di Azione per la Società dell'Informazione e nel Piano di e_Government conformandole alle esigenze ed alle priorità specifiche della Puglia.

A.1.2 Motivazioni

La decisione di realizzare la RUPAR Puglia rientra nella strategia della Regione per lo sviluppo e la diffusione della Società dell'Informazione.

La Società dell'Informazione è uno degli obiettivi prioritari del programma del governo regionale in considerazione dell'importanza che il nuovo modello di società, più partecipato ed aperto, riveste per il futuro della Puglia.

Solo con il concorso dei nuovi stili di vita e delle nuove tecnologie che caratterizzano la Società dell'Informazione è possibile ipotizzare di poter realizzare con successo alcuni obiettivi strategici che il governo regionale si è posto, tra questi:

- la realizzazione del sistema Puglia inteso come azione coordinata dei soggetti attivi sul territorio (le associazioni di categoria, le Università, le Camere di Commercio, le pubbliche amministrazioni, ecc;
- l'innovazione del sistema della formazione ed una maggiore circolazione delle idee e dei saperi nella regione;

- l'innovazione dell'apparato produttivo e commerciale regionale;
- il miglioramento della capacità dei settori distintivi dell'economia regionale di operare "in rete", in modo da rafforzarne la competitività a livello nazionale e internazionale come sistemi economici integrati;
- la tutela e la valorizzazione delle risorse ambientali, artistiche e culturali locali;
- la modernizzazione degli enti e dei servizi pubblici al fine di accelerare e rendere effettivo il processo di decentramento funzionale e di razionalizzazione della Pubblica Amministrazione;
- la promozione integrata del territorio, de prodotti e delle imprese pugliesi nel mondo;
- la collaborazione-competizione virtuosa con gli altri sistemi territoriali.

Peraltro, lo sviluppo e la diffusione della Società dell'Informazione è per molte ragioni una meta obbligata per non restare indietro sul piano della innovazione e della competitività con gli altri sistemi territoriali e per non rischiare di diventare un puro mercato di sbocco per beni e servizi ideati e prodotti altrove.

La situazione attuale caratterizzata da una limitata dimestichezza delle imprese, degli enti pubblici e dei pugliesi con le nuove tecnologie non scoraggia certamente la Regione da intraprendere una strategia per la Società dell'Informazione ragionevolmente ambiziosa con la quale intende, non solo colmare il ritardo esistente, ma anche promuovere lo sviluppo in loco di prodotti, ser-

vizi ed imprese della “nuova economia” in grado di competere sul mercato globale.

Questo percorso, sicuramente non agevole, appare praticabile in considerazione della presenza in Puglia di numerosi centri di eccellenza nel settore ICT e di un vivace tessuto di piccole e medie imprese desiderose di affermarsi anche fuori dei confini regionali.

Il progetto RUPAR nasce dall’urgenza di anticipare gli interventi sicuramente utili per l’attuazione del Piano per la Società dell’Informazione, previsto dalla Misura 6.2 del POR.

Le reti telematiche hanno infatti nella Società dell’Informazione un ruolo paragonabile per importanza a quella che hanno le tradizionali infrastrutture di trasporto fisico: strade, autostrade, ferrovie, porti, aeroporti, ecc.

La RUPAR, oltre a costituire una infrastruttura telematica al servizio del territorio, consente di attaccare uno dei settori più importanti per la Società dell’Informazione, quello che riguarda la Pubblica Amministrazione.
Si deve considerare infatti che la modernizzazione della Pubblica Amministrazione è diventata un obiettivo strategico preteso dai contribuenti e perseguito dal Governo del Paese, dato che costituisce una condizione essenziale per la modernizzazione dell’intero sistema produttivo e sociale del Paese.

Lo stato delle autonomie locali pugliesi non si discosta dagli altri settori dell'economia pugliese. Secondo le più recenti indagini la Puglia è, in materia di modernizzazione dei servizi pubblici, ai primi posti tra le regioni del Mezzogiorno ma accusa evidenti ritardi rispetto alle Regioni del Centro e del Nord Italia che a loro volta, salvo qualche eccezione, non sono certo all'avanguardia in Europa.

La RUPAR costituisce un primo importante passo in avanti verso l'innovazione degli enti pubblici perché realizza i servizi di base per lo scambio e la condivisione telematica di informazioni e lo sviluppo di servizi applicativi più complessi che interesseranno sia i processi interamministrativi che le prestazioni agli utenti finali.

Ad esempio, potranno essere realizzate applicazioni infotelematiche che consentiranno lo scambio e l'aggiornamento automatico di archivi e documenti tra amministrazioni diverse, la semplificazione ed il monitoraggio di procedure che interessano più enti, la completa informatizzazione degli sportelli unici al cittadino ed alle imprese.

La scelta di iniziare dalla Pubblica Amministrazione è quindi motivata da una duplice esigenza: quella di trasformare le pubbliche amministrazioni pugliesi in enti in grado di pianificare, promuovere e coordinare lo sviluppo operando in modo coordinato nel pieno rispetto delle autonomie e quella di far sì che le amministrazioni stesse diventino modello e volano dell'utilizzo e

dello sviluppo di servizi e relazioni tipiche della Società dell'Informazione.

Attraverso il progetto RUPAR, inoltre, la Puglia si inserisce a pieno titolo in iniziative di rilevanza nazionale, quale l'interconnessione alla RN, cogliendo appieno le opportunità, prima tra tutte quella di stabilire utili rapporti di collaborazione con il Centro Tecnico della Rete Nazionale e con le altre Regioni per lo scambio di conoscenze ed esperienze tecniche.

La RUPAR Puglia, in modo analogo alla RUPA ed alla RN, si configura non come una nuova infrastruttura fisica di comunicazione ma come la qualificazione e la organizzazione dei servizi Internet già commercialmente disponibili. Questo consente già di per sé di aumentare la domanda di servizi telematici, di corroborare le imprese locali operanti nel settore dei servizi Internet e di calmierare le tariffe in favore anche dell'utenza privata, professionale e non.

Il campo d'azione della RUPAR Puglia è il Sistema degli Enti Locali della Puglia che comprende le Province, i Comuni, le Comunità Montane, le ASL e le AO, ma i nuovi servizi telematici saranno disponibili via Internet per cittadini ed imprese, anche fuori dai confini regionali.

L'intento della Regione Puglia è di promuovere la Società dell'Informazione partendo dalla modernizzazione del settore pubblico cogliendo anche l'obiettivo di trasformare questo settore da freno a propulsore dello sviluppo.

I nuovi servizi telematici, interni ed esterni, della Pubblica Amministrazione sono lo scopo principale della **RUPA**, della **RN**, delle **RUPAR** e delle **Community Network**.

Alcuni di questi servizi sono stati già identificati dal Piano di e_Government e dal POR Puglia, altri rivengono dalle iniziative di informatizzazione già realizzate dalla Regione stessa e che potranno beneficiare dei servizi di rete della RUPAR, tra questi:

- il Sistema informativo Sanitario Regionale;
- il Sistema informativo per il Monitoraggio degli Interventi Regionali (MIR);
- il Sistema di gestione telematica dell'iter delle delibere della Giunta della Regione Puglia (CIFRA);
- il Sistema informativo dell'Agricoltura (SITAMA);
- il Sistema di sottomissione dei Piani di Miglioramento Aziendale (PMA) per le aziende agricole
- il Sistema informativo del Lavoro (SIL);
- il Sistema Informativo della Protezione Ambientale (SIPA);
- il Sistema integrato telematico dei porti turistici;
- il Sistema informativo dei beni culturali;

- Sistema informativo per il monitoraggio della attività produttive (SIMAP);
- Sistema informativo dell'osservatorio della finanza locale;
- Servizi telematici di interscambio catasto-comuni;
- i Portali informativi per l'accesso via Internet e la navigazione delle basi di dati della Pubblica Amministrazione;
- i Portali per l'erogazione via Internet di servizi ai cittadini ed alle imprese;
- i Portali informativi sui dati di interesse regionale;
- il Portale per i servizi all'impiego per consentire l'incontro tra domanda ed offerta di lavoro per via telematica.

A.1.3 Obiettivi

Con il progetto RUPAR la Regione Puglia realizza e rende disponibile una infrastruttura telematica, stabile, veloce, affidabile, sicura ed economicamente conveniente, per il collegamento e la comunicazione tra le istituzioni pubbliche regionali e, attraverso la Rete Nazionale, tra queste e le Amministrazioni dello Stato e delle altre Regioni.

I numeri della RUPAR sono indicativi della sua complessità:

- **350 Enti** serviti tra cui le cinque Amministrazioni provinciali ed i cinque Comuni capoluogo, 258 Comuni, 6 Comunità montane, 12 Aziende sanitarie (ASL), 5 Aree di Sviluppo Industriale (ASI), l'Agenzia regionale per il lavoro, 6 Consorzi di Bonifica, l'Agenzia Regionale per la Protezione dell'Ambiente (ARPA) e 2 Enti Parco;
- **20.000 utenti** direttamente serviti: amministratori, dirigenti e dipendenti degli Enti collegati;
- **10.000 Km**. di estensione complessiva della rete;
- **350 Km**. di distanza tra le due utenze più lontane;
- Velocità di trasferimento dati da **64Kbps** ai **2 Mbps** in funzione della quantità di traffico generato dai singoli Enti;
- **10.000 certificati** individuali di firma digitale rilasciati a Presidenti, Sindaci, Assessori, Consiglieri e dirigenti delle Amministrazioni.

L'investimento previsto nei cinque anni è di 88Mld di Lire (**45.000.000 di Euro**). **Per le Amministrazioni collegate non è previsto alcuno onere**. Il 50% dell'investimento è finanziato dal POR, ed il restante 50% dai fornitori dei servizi. Queste società potranno rientrare del loro investimento con la vendita alle Amministrazioni di servizi aggiuntivi, non catalogati tra quelli basilari della RUPAR, e con il mantenimento dei servizi negli anni successivi.

Sotto l'aspetto architetturale la RUPAR Puglia è organizzata a grandi linee in cinque nodi principali, detti **EPO** (**E**xchange **P**oint **O**perator), ubicati nei capoluoghi di provincia, ai quali si collegano le reti delle singole Amministrazioni. Tali EPO saranno **Locali** e **Privati**, identificati dalla sigla **EPO-LP**, cioè **esclusivamente riservati** alla RUPAR Puglia e di conseguenza non gestiti come punti di interconnessione riconosciuti dall'intero mondo Internet. Di seguito si utilizzerà indifferentemente la sigla EPO oppure EPO-LP per riferirsi ai nodi di interscambio totalmente riservati alla RUPAR Puglia.

Ad esempio, la rete del Comune di Gallipoli si collegherà all'EPO di Lecce, quella del Comune di Manfredonia all'EPO di Foggia, e così via. L'EPO di Bari svolge funzioni di smistamento del traffico interprovinciale e di nodo di erogazione dei servizi resi disponibili a livello regionale centrale.

Tanti **Centri di Gestione** (CG) quanti sono i fornitori che gestiscono le reti delle Amministrazioni: un Centro di Gestione può servire più amministrazioni.
Un **Centro Tecnico** (CT) che coordina e controlla l'attività dei Centri di Gestione e provvede al collegamento con la Rete Nazionale.

La RUPAR, nel suo complesso, fornisce alle Amministrazioni i seguenti servizi:

- Il servizio di trasporto dati che realizza materialmente il collegamento tra le Amministrazioni;

- I servizi di interoperabilità di base che consentono di svolgere le funzioni fondamentali di scambio di informazioni (posta elettronica, trasferimento file, accesso ad Internet, ecc.) ed ai tecnici di gestire gli aspetti operativi e sistemistici della rete (indirizzamento dei calcolatori e degli utenti della rete, autorizzazioni, calcolo dei tempi di connessione alla rete, ecc.);
- I servizi di firma digitale per firmare atti e documenti elettronici;
- I servizi di cooperazione applicativa, che forniscono le funzionalità di base per lo sviluppo ed il funzionamento di quelle applicazioni che richiedono il concorso di più Amministrazioni. Esempi di queste applicazioni, dette cooperative, sono: il Sistema Sanitario Regionale per la gestione integrata dei dati clinico-sanitari e l'integrazione tra l'anagrafe sanitaria e quella comunale; l'Osservatorio della finanza locale per la verifica della efficacia e della efficienza della spesa pubblica; il sistema Catasto-Comuni per l'interscambio di informazioni tra amministrazione centrale (Catasto) ed amministrazioni locali (Comuni);
- I servizi di gestione operativa e sistemistica, sicurezza, manutenzione, assistenza e supporto tecnico svolti dai Centri di Gestione e dal Centro Tecnico.

Il servizio di trasporto dati ed i servizi di interoperabilità di base sono forniti alle singole Amministrazioni da fornitori esterni, scelte dalle Amministrazioni, da un elenco di fornitori qualificati e certificati dal CT, a condizioni tecniche prestabilite.

Una Amministrazione avrà un **unico** fornitore (FSR, Fornitore Servizi RUPAR) per entrambi i servizi di Trasporto ed Interoperabilità.

A.1.4 Strumenti

La realizzazione ed il funzionamento della RUPAR viene garantita attraverso un insieme coordinato di strumenti di carattere procedurale, organizzativo e tecnico.

Per lo sviluppo ed il funzionamento della RUPAR sono previste tre fasi:

- la fase di pianificazione
- la fase di attuazione
- la fase di esercizio e controllo

La fase di pianificazione identifica e stabilisce:

- i servizi della RUPAR e gli enti che possono collegarsi
- il traffico atteso, il dimensionamento, l'architettura tecnica ed organizzativa della rete

- le politiche di sicurezza adottate e gli standard tecnici di riferimento per lo sviluppo ed il funzionamento della rete e dei servizi
- le responsabilità ed i ruoli dei soggetti coinvolti nello sviluppo, nell'esercizio e nell'utilizzo della rete e dei servizi
- le modalità di adesione da parte degli enti
- le previsioni di spesa ed i criteri per la copertura dei costi
- il piano temporale per l'attivazione dei servizi

I risultati della pianificazione, per come è stata impostata alla data di redazione del presente documento, sono raccolti nel Capitolo D Attivazione e esercizio del documento e sottoposti alla validazione della Regione Puglia.

Dopo la fase di pianificazione, è prevista la fase di attuazione che comprende:

- la costituzione del Centro Tecnico;
- la gara per la qualificazione dei Fornitori dei Servizi RUPAR (FSR) per i servizi di Trasporto ed Interoperabilità;
- la gara per la qualificazione dei Fornitori dei Servizi di Firma Digitale (FSFD);
- la gara per la fornitura della strumentazione del Centro Tecnico;
- la pubblicazione dell'elenco dei fornitori qualificati;
- la fornitura della strumentazione e l'allestimento del Centro Tecnico e degli EPO ;

- la fornitura e l'attivazione dei servizi.

Completate queste attività, è prevista la fase di esercizio durante la quale:

- il Centro Tecnico inizia a erogare servizi tecnologici (p. es. gestione EPO-LP);
- le singole Amministrazioni appaltano il servizio di trasporto ed i servizi di interoperabilità;
- i FSR allestiscono i Centri di Gestione e collegano le Amministrazioni alla RUPAR;
- le Amministrazioni, una volta collegate, iniziano ad utilizzare i servizi di trasporto e di interoperabilità e, successivamente, i servizi di firma digitale e di cooperazione applicativa, questi ultimi per lo sviluppo di nuovi servizi applicativi alla utenza che, in definitiva, sono il principale valore aggiunto della RUPAR;
- la Regione Puglia inizia alcuni progetti applicativi significativi previsti nell'ambito del POR, quali p.es. Catasto-Comuni e Osservatorio della Finanza Locale.

Le Amministrazioni possono rivolgersi:

- ai Centri di Gestione per sottoporre domande o segnalare malfunzionamenti e cattivi funzionamenti della rete;
- al Centro Tecnico per consulenze o richieste di controlli della qualità del servizio.

I Centri Gestione provvedono alla sorveglianza dei servizi erogati, al salvataggio dei dati dell'utenza in modo da poterli ripristinare in caso di danneggiamento o perdita, ad intervenire in modo tempestivo per la soluzione di eventuali problemi, a raccogliere e registrare le informazioni sulla attività svolta sulla rete da parte dell'utenza.

Il Centro Tecnico provvede a gestire una banca dati in cui sono contenute le domande e le segnalazioni degli utenti e gli interventi dei Centri di Gestione ed ad elaborare sulla base di questi dati report statistici della qualità complessiva del servizio della RUPAR.

Strumenti Organizzativi

Oltre gli enti coinvolti nell'attuazione delle misure del POR (la Giunta regionale, l'Area di Coordinamento delle Politiche Comunitarie e l'ufficio di Presidenza della Giunta, in qualità di responsabile della Misura 6.3 del POR che riguarda la RUPAR), la pianificazione, l'attuazione ed il controllo della RUPAR richiedono la presenza di strutture specialistiche. Queste sono:

- il Centro Tecnico (CT);
- le unità responsabili dei **Servizi Informatici** delle **Amministrazioni** che aderiscono alla RUPAR (**SI-Amm**);

- i **Centri** di **Gestione** dei **Servizi RUPAR** (**CG-SR**);
- i Centri Servizi.

Il Centro Tecnico (CT) della RUPAR, ruolo svolto da Tecnopolis come stabilito nei Complementi di Programmazione del POR, rappresenta il braccio operativo e tecnologico della Regione per il governo della RUPAR. E' costituito da specialisti in informatica e telematica, attrezzati con le necessarie apparecchiature, e provvede:

- alla pianificazione ed al controllo dell'efficacia e dell'efficienza della rete;
- alla definizione degli standard tecnici, gestionali ed economici, vincolanti per chi voglia operare nella RUPAR;
- alla certificazione dei fornitori dei servizi di trasporto ed interopeabilità (FSR);
- al coordinamento ed al controllo delle attività dei FSR;
- alla definizione delle politiche di sicurezza ed al controllo dell'attuazione delle stesse;
- alla gestione dei nodi di interscambio della rete (EPO-LP);
- alla gestione ed al controllo complessivo della RUPAR;
- alla supervisione dei collegamenti a livello RN/RUPA ed ai rapporti con il Centro Tecnico della RN;

- alla progettazione, sviluppo e gestione dei servizi di supporto per la cooperazione applicativa.

Le unità responsabili dei Servizi Informatici di ciascuna Amministrazione (SI-Amm) coordinano, gestiscono e controllano i sistemi informativi e le reti del proprio ente. Sovrintendono direttamente il lavoro del FSR scelto dalla propria Amministrazione, si rivolgono al CT per specifiche consulenze e/o richieste di controlli della qualità del servizio.

A.2 Descrizione dei servizi

La RUPAR ha per finalità l'interconnessione delle diverse Amministrazioni con una infrastruttura di servizio che garantisca la massima efficienza, riservatezza ed affidabilità.

La generica definizione di servizio di interconnessione è meglio specificata distinguendo tra le seguenti tipologie di servizi:

A.2.1 Servizio di trasporto

Concerne le funzionalità di trasporto ed instradamento dei flussi di dati da una Amministrazione e l'altra. La tecnologia di riferimento per questo servizio è quella della rete **Internet** e quindi i **protocolli TCP/IP**, in questo caso il servizio di trasporto viene denominato "**Servizio IP**".

A.2.2 Servizio di interoperabilità di base

Concerne le funzionalità basilari di accesso alle informazioni da una Amministrazione all'altra. Le funzionalità di riferimento sono anche in questo caso derivate dalla rete Internet e sono suddivisibili a loro volta in due principali classi: "*Interoperabilità applicativa*" ed "*Interoperabilità tecnica*". Alla prima apparten-

gono i servizi diretti utilizzati dagli utenti di una Amministrazione per effettuare uno scambio informativo con un'altra Amministrazione:

- posta elettronica
- accesso a WorldWideWeb
- trasferimento file
- terminale virtuale
- accesso a News

Alla seconda appartengono i servizi utilizzati dagli utenti in modo indiretto, oppure messi a disposizione dalla infrastruttura stessa a fini di gestione e supporto:

- nomi di dominio (DNS)
- directory
- tempo ufficiale di rete
- gestione sistemi e rete
- sicurezza (Firewall/Proxy)

A.2.3 Servizi di Firma Digitale

Concernono la possibilità di conferire valore legale ad atti e transazione di tipo elettronico in modo perfettamente analogo agli atti e transazioni di tipo cartaceo fisicamente firmati dall'esecutore.

L'utilizzo più immediato di queste funzionalità lo si può avere nello scambio di informazioni mediante Posta Elettronica che, essendo un servizio di interoperabilità di base, sarà immediatamente disponibile all'avvio della RUPAR anche in assenza di specifiche applicazioni cooperative, le quali presumibilmente seguiranno dopo un certo lasso di tempo dall'avvio della rete.

A.2.4 Servizi di supporto

Concernono tutti i servizi complementari a quelli principali, che concorrono al livello qualitativo complessivo del servizio così come è percepito dall'utente: p. es. Help Desk, accounting etc.

A.2.5 Servizi di cooperazione applicativa

Concernono le funzionalità di livello più alto in quanto rappresenta, più che un semplice accesso alle informazioni, come avviene nel caso dei servizi di interoperabilità di base, una reale integrazione delle applicazioni informatiche di diverse Amministrazioni.

Esempi di applicazioni informatiche che potranno essere realizzate sulla RUPAR sfruttando i servizi di cooperazione applicativa sono:

- Il Sistema di Interscambio tra Catasto e Comuni per la gestione integrata delle informazioni catastali e territoriali
- Il Sistema Sanitario Regionale, per la gestione integrata dei dati clinico-sanitari nonché per l'integrazione tra l'anagrafe sanitaria e quella comunale
- L'Osservatorio della finanza locale, che integri i dati della spesa della PAL con le informazioni relative allo sviluppo del territorio collegato alla spesa

Essi sono previsti, unitamente allo sviluppo della RUPAR, nella misura 6.3 del POR 2000-2006 della Regione Puglia.

A.3 Architettura della rete

A.3.1 Descrizione

La seguente figura illustra come l'architettura funzionale della RUPAR sia rappresentabile con un modello a strati costituiti dai tre principali livelli funzionali precedentemente descritti.

L'interazione tra le Amministrazioni A e B è a livello di interoperabilità di base, mentre quella tra C e D è a livello di cooperazione applicativa. In entrambi i casi sono utilizzati i servizi di trasporto e l'interazione a livello di cooperazione applicativa fa anche uso dei servizi di interoperabilità di base.

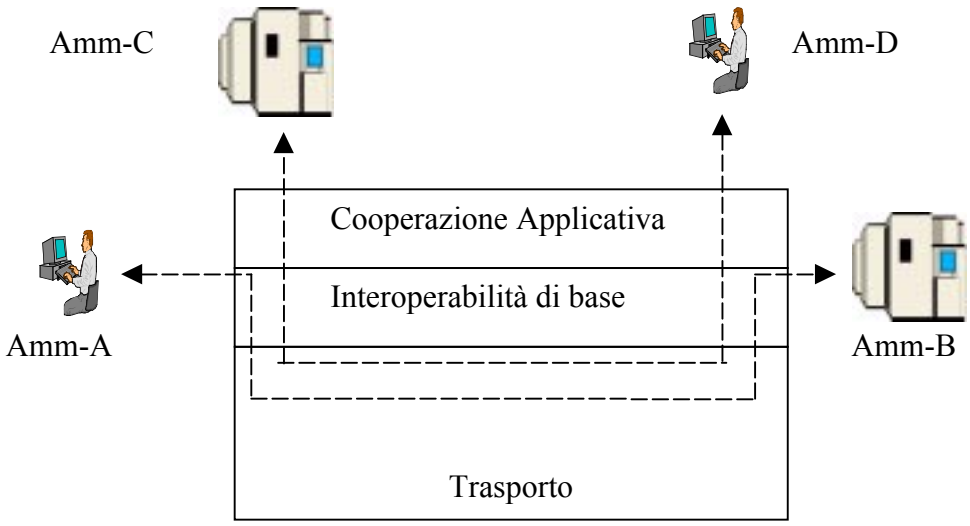


Figura 1. Architettura funzionale

Poiché l'interazione ad un livello più alto utilizza sempre i livelli sottostanti, ne consegue che l'obiettivo primario dello sviluppo della RUPAR è quello di realizzare in modo completo dal punto di vista funzionale e della distribuzione territoriale (capillarità) i primi due livelli funzionali, lasciando a specifici progetti il compito di realizzare la cooperazione applicativa in specifici campi.

A.3.1.1 Schema tecnico generale

La realizzazione dei primi due livelli di servizio dell'architettura della RUPAR si baserà sullo schema generale illustrato nella seguente figura.

In questo schema le reti interne di ogni Amministrazione sono indicate come "Dominio Amministrazione ..." (in termini correnti esse sono delle reti "Intranet" delle Amministrazioni) e sono interconnesse dalla rete di trasporto della RUPAR (che può essere definita una Extranet delle PAL) che a sua volta è interconnessa ad altre Community Network mediante la Rete Nazionale e la rete Internet.

La RUPAR è gestita e controllata dal punto di vista operativo dai **Centri di Gestione**: i Centri di Gestione dei Servizi RUPAR (CG-SR) attivati e gestiti dai Fornitori.

Il **Centro Tecnico** (CT) di gestione e controllo complessivo della RUPAR svolge anche funzioni di pianificazione, controllo della qualità dei servizi e definizione degli standard tecnici.

Ogni Amministrazione individuerà al proprio interno una funzione denominata **Servizio Informatico** dell'**Amministrazione** (**SI-Amm**) per gestire il rapporto con la RUPAR.

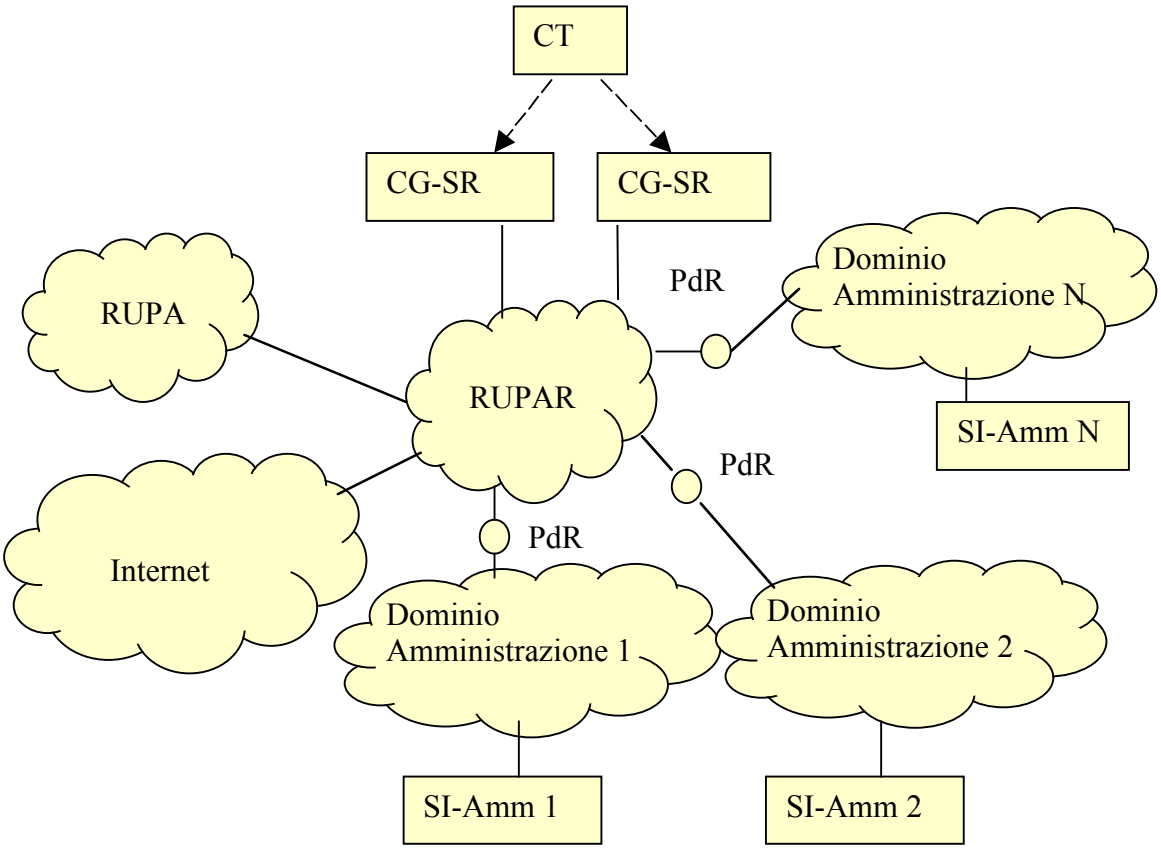


Figura 2. Schema generale della RUPAR

L'interconnessione tra il Dominio di un'Amministrazione e la RUPAR è generalmente denominata **Porta di Rete** (**PdR**) e contiene sia l'interconnessione a livello di trasporto che a livello di interoperabilità di base.

L'interconnessione a livello di trasporto distingue tra i circuiti su cui viene instradato il traffico di cooperazione tra le Pubbliche Amministrazioni (Extranet della PA) ed i circuiti sui quali viene instradato il traffico da e verso la rete Internet e quindi verso altre **Community Network**.

La figura seguente schematizza questi due tipi di circuiti che vanno intesi come circuiti virtuali, non fisici, coesistenti sulla linea che interconnette la PdR di un'Amministrazione alla RUPAR.

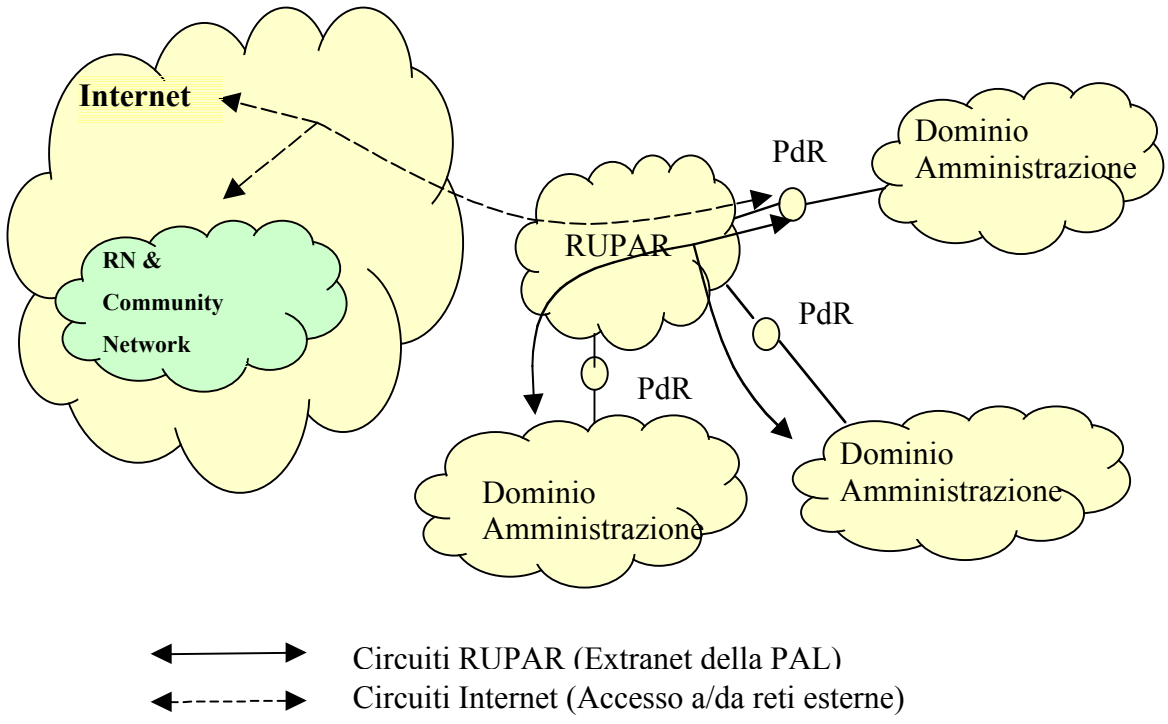


Figura 3. Tipi di circuiti per un'Amministrazione

I due tipi diversi di circuiti sono tenuti rigorosamente distinti a livello RUPAR, dato che la rete Extranet delle PAL, sulla quale si svolge il traffico di interoperabilità e cooperazione tra le diverse Amministrazioni, deve essere non raggiungibile dalla rete Internet (si tratta di una rete privata riservata alle PAL) per motivi di sicurezza.

L'unico punto di contatto tra questi due tipi di circuiti è nella **PdR** dove vengono esplicate le politiche di sicurezza prescritte nel seguito del presente documento, in corrispondenza della descrizione dei Servizi di Interoperabilità di base.

A.3.1.2 Struttura Organizzativa generale

Il seguente Diagramma mostra il **flusso delle interazioni organizzative** tra questi soggetti: il CT risponde alla Regione Puglia dell'intera infrastruttura e coordina e controlla le attività dei CG-SR.

Gli SI-Amm normalmente hanno rapporti con i CG-SR per tutte le attività di normale amministrazione, ma possono rivolgersi a CT per specifiche consulenze e/o richieste di controlli della qualità del servizio.

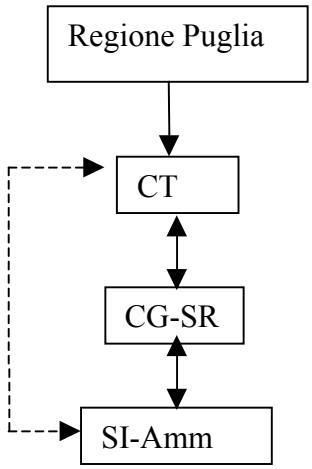


Figura 4. Diagramma flusso organizzativo

A.3.1.3 Requisiti prestazionali

Va sottolineato che in molti casi i servizi di cooperazione applicativa possono richiedere, per poter essere fruiti in modo efficiente, una interconnessione locale, almeno a livello provinciale, ad alta velocità.

E' questo il caso, per esempio, del servizio di cooperazione applicativa di Interscambio tra Catasto e Comuni che si basa su un'architettura di Centri Servizi che servono raggruppamenti di Comuni della stessa provincia: poiché questo tipo di applicazione tratta basi dati di tipo anche cartografico e di mole non indifferente, le prestazioni della rete a livello locale sono un parametro molto importante.

Da questo esempio si possono far discendere degli importanti parametri qualitativi, che possono essere riassunti nelle seguenti asserzioni:

- il servizio di trasporto a livello locale (provinciale) deve garantire una interconnessione senza limitazioni di banda (rispetto alla velocità dei collegamenti delle Amministrazioni collegate): in sintesi "***Full bandwith***"
- il servizio di trasporto a livello geografico (regionale) deve poter essere contrattualizzato da una Amministrazione con una precisa qualità di connessione **BMG** (**B**anda **M**inima **G**arantita) verso tutti gli altri soggetti collegati e verso i servizi di collegamento ad altre comunità di PA e ad Internet

A.3.2 Modello realizzativo

Il modello realizzativo della RUPAR Puglia prevede che la Regione selezioni dei Fornitori, abilitandoli così ad offrire i propri servizi. L'insieme dei servizi (di Trasporto, di Interoperabilità e di Firma Digitale) è quindi liberamente offerto alle Amministrazioni che ne facciano richiesta ai Fornitori selezionati, i quali supportano i servizi sulla propria infrastruttura tecnologica a livello regionale opportunamente interconnessa con quella degli altri fornitori in un'ottica di reti federate.

Questo **modello** realizzativo, definito "**Aperto**", in quanto prevede che i servizi siano erogati da più fornitori in concorrenza tra di loro, è stato preferito al modello, peraltro adottato in altre RUPAR regionali, che prevede la selezione di un unico fornitore per ogni classe di servizio.

E' opportuno inoltre fare le seguenti considerazioni:

- I servizi di trasporto e di interoperabilità, pur essendo caratterizzati da una certa differenziazione tecnica e funzionale, essendo i primi più specificatamente orientati al mondo delle telecomunicazioni ed i secondi al mondo dell'informatica, possono essere visti come servizi integrati tenendo conto della progressiva ed inarrestabile integrazione reciproca di questi due mondi, sintetizzata dal termine "Telematica", non v'è dubbio quindi che un fornitore possa tranquillamente fornire entrambe le classi di servizi
- Viceversa i servizi di Firma Digitale hanno una specificità tecnologica, organizzativa e formale (iscrizione all'albo delle Certification Authority AIPA) che li differenziano in modo sostanziale dai servizi di trasporto e da quelli di interoperabilità di base

In considerazione di ciò, è quindi opportuno, al fine di realizzare un modello "Aperto" nel quale non ci siano però un numero di variabili troppo elevato il che potrebbe indurre a disordine, prevedere che siano abilitati dei Fornitori che offrano e supportino sia il Servizio di Trasporto che il Servizio di Interoperabilità ed inoltre degli altri Fornitori che offrano e supportino il Servizio di Firma Digitale

La realizzazione della RUPAR Puglia significa:

- Dal punto di vista dei Servizi di Trasporto e Servizi di Interoperabilità selezionare dei fornitori (FSR, Fornitori Servizi RUPAR) che siano in grado di realizzare sulle proprie infrastrutture di comunicazione una rete privata virtuale con tecnologia TCP/IP dedicata esclusivamente a collegare gli enti della PA regionale. L'esito della selezione non è quindi la costituzione di una infrastruttura di proprietà regionale (anche se vi sono Regioni che hanno intrapreso questa strada), bensì un convenzionamento con i fornitori sulla fornitura di un servizio di trasporto a condizioni standard garantite e omogenee sul territorio regionale per gli enti locali che di volta in volta ne faranno richiesta. Inoltre detti Fornitori dovranno essere dotati della necessaria competenza tecnica e delle infrastrutture tecnologiche atte alla fornitura di tutti i servizi di interoperabilità di base (sia di tipo applicativo che di tipo tecnico) descritti nel paragrafo 2 del presente documento.

- Dal punto di vista dei Servizi di Firma Digitale selezionare dei Fornitori (FSFD, Fornitori Servizi Firma Digitale) che siano qualificati tecnicamente e formalmente (Autorità di Certificazione approvate dall'AIPA)

Partendo da queste premesse la RUPAR sarà realizzata seguendo questo approccio:

1. effettuazione di Gare di selezione distinte per i due diversi gruppi di Fornitori (FSR e FSFD);
2. selezione dei gruppi di fornitori abilitati ad offrire i propri servizi su RUPAR;
3. attivazione, da parte dei Fornitori selezionati, delle relative infrastrutture di servizio sotto il coordinamento del CT;
4. adesione degli Enti utenti finali alla RUPAR, mediante un processo di scelta, all'interno dell'Albo dei Fornitori selezionati, di quello più idoneo.

In questo modello realizzativo il CT ha i seguenti compiti:

- emanare gli standard tecnici, gestionali ed economici, che sono vincolanti per chi voglia operare nella RUPAR;
- certificare i fornitori, abilitandoli così ad offrire i servizi;
- gestire i nodi di interazione della rete (EPO-LP, cfr. paragrafo successivo);

- gestire il collegamento ad altre Community Network e ad altre RUPAR;
- gestire l'accesso via Internet ai servizi centrali della RUPAR (p. es. Portale della RUPAR Puglia);
- controllare che l'interazione tra fornitori avvenga secondo le modalità previste, garantendo così la qualità complessiva del servizio offerto dalla RUPAR;
- interagire con i Centri di Gestione dei fornitori al fine effettuare il monitoraggio in tempo reale dello stato dei servizi;
- effettuare gli *audit* di sicurezza e impenetrabilità dei servizi della PAL per verificare che siano correttamente attuate dai fornitori le politiche di sicurezza prescritte.

A.3.3 Struttura tecnica

L'insieme dei servizi di trasporto e di interoperabilità è liberamente offerto dai Fornitori certificati che supportano i servizi sulla propria infrastruttura tecnologica a livello regionale ed inoltre forniscono la connettività ad Internet per le PAL ad essi collegate.

Dal punto di vista tecnologico la qualità del servizio di trasporto in questo assetto normativo ed organizzativo può essere garantita solo fissando delle regole tecniche di interconnessione tra i Fornitori.

La principale regola è che l'interconnessione tra le reti dei Fornitori, al solo fine di smistare il traffico RUPAR, avvenga attraverso strutture dedicate ad alte prestazioni definite **EPO-LP** (**E**xchange **P**oint **O**perator – **L**ocale **P**rivato).

Le gestione degli EPO-LP sarà a carico del CT.

L'infrastruttura di trasporto deve avere una distribuzione sul territorio che consenta di coprire le cinque province con una capacità di trasporto ad alta velocità e con elevate caratteristiche di continuità di servizio (*uptime*).

A questo fine si prevede che essa abbia cinque nodi principali di concentrazione e di snodo del traffico, allocati nei cinque capoluoghi di provincia.
Il nodo di Bari svolgerà primariamente, oltre al servizio per la provincia di Bari, funzioni di smistamento del traffico interprovinciale e di nodo di erogazione dei servizi resi disponibili a livello regionale centrale.

Il dimensionamento dell'infrastruttura dovrà essere adeguato a supportare i flussi di dati verso il nodo principale di Bari sia in condizioni normali che in condizioni di guasto su un collegamento.

Inoltre ogni nodo provinciale dovrà supportare l'instradamento del traffico a banda piena (*Full Bandwith*) tra Amministrazioni collegate allo stesso nodo.

I servizi di interoperabilità potranno essere erogati:

- presso la connessione fisica con la RUPAR della rete di dominio di un'Amministrazione ad opera di un FSR
- in strutture dedicate (Centri Servizi di Interoperabilità) connesse a RUPAR, per mezzo delle quali un FSR offre i suoi servizi ad una pluralità di Amministrazioni le cui reti di dominio si collegano al Centro Servizi in modo trasparente

A.4 Responsabilità e ruoli

La RUPAR prevede la partecipazione di una pluralità di soggetti a ciascuno dei quali sono richieste precise mansioni e responsabilità e la disponibilità ad operare in una logica fortemente collaborativa.

Un ruolo preminente è svolto dalla **Regione Puglia** che oltre ad essere uno degli utenti della RUPAR è anche l'Amministrazione che promuove, organizza e sostiene sia sul piano tecnico che su quello finanziario il progetto.

Un ruolo non meno importante è svolto dalle altre **Amministrazioni locali** della Puglia. Il loro intervento è determinante sia per la realizzazione della infrastruttura di rete che per la progettazione e lo sviluppo dei servizi telematici per i cittadini e le imprese pugliesi.

Gli aspetti più propriamente tecnici della RUPAR sono invece affidati alle imprese che operano nel settore delle telecomunicazioni e dei servizi Internet ed al **Centro Tecnico** della RUPAR che svolge per conto della Regione le attività tecnico informatiche di progettazione, coordinamento e controllo. La RUPAR è infatti una rete che prevede il concorso di **più fornitori** (*multi-provider*) le cui attività sono coordinate e controllate dal Centro Tecnico.

Nel progetto i fornitori di servizi svolgono anche il ruolo di cofinanziatori del progetto. E' finanziato dalla Regione Puglia, direttamente e per tramite del POR2000-2006, solo il **50%** del costo dei servizi prestati. Il restante 50% è inteso come investimento che le aziende recupereranno con la vendita di servizi aggiuntivi alle Amministrazioni e più in generale da un aumento significativo della domanda di servizi da parte di aziende private, enti pubblici, utenze professionali e familiari che la RUPAR determinerà.

Le funzioni del Centro Tecnico sono affidate al Parco Scientifico Tecnopolis CSATA che allo stato attuale garantisce progetti e soluzioni scientificamente rilevanti ed indipendenza di giudizio rispetto ai fornitori di servizi telematici.

A.4.1 La Regione Puglia

La Regione Puglia promuove, sostiene e coordina il progetto RUPAR secondo le logiche del decentramento e del federalismo. La stessa rete è considerata propedeutica e funzionale allo sviluppo di servizi applicativi per il decentramento dalla Regione agli Enti Locali di funzioni amministrative e per una maggiore coesione del Sistema delle Autonomie Locali pugliesi.

Nel progetto la Regione riconosce agli Enti Locali un ruolo non solo di utente finale beneficiario dei risultati e delle provvidenze della iniziativa, ma anche di protagonista attivo nella realizzazione dei servizi applicativi a valore aggiunto offerti sulla Rete.

Nello stesso tempo tutela e rispetta l'autonomia delle singole Amministrazioni locali per le scelte che riguardano i loro sistemi informatici e le loro reti interne.

La Regione sostiene il progetto svolgendo le attività di indirizzo e vigilanza della Rete, di realizzazione ed erogazione dei servizi generali, compreso il collegamento alla Rete Nazionale, e di assistenza tecnica alle Amministrazioni locali. Le risorse finanziarie utilizzate sono quelle previste dalla Misura 6.3 del POR Puglia.

Le funzioni politiche di indirizzo e vigilanza sono svolte dalla Presidenza della Giunta Regionale. La gestione del progetto è svolta dall'Ufficio di Presidenza.

La Presidenza provvede a determinare finalità ed obiettivi della RUPAR e ad adottare le misure legislative, regolamentari ed amministrative necessarie per il loro conseguimento. Provvede inoltre a trattare, nell'ambito della Conferenza Stato-Regioni, le questioni inerenti l'interscambio di dati ed informazioni e lo sviluppo di nuovi servizi telematici che richiedono il concorso di più Amministrazioni, a livello centrale e locale,ed a stipulare accordi diretti con altre Amministrazioni ed aziende.

L'**Ufficio di Presidenza** provvede a:

- supportare tecnicamente la Presidenza ed ad attuare gli indirizzi da essa definiti;
- organizzare le attività di promozione e diffusione della Rete e di consultazione delle amministrazioni locali, delle forze sociali, economiche e culturali e delle associazioni dei cittadini;
- organizzare modalità di coordinamento e di cooperazione tra le Amministrazioni locali pugliesi, con le altre regioni e con il Governo centrale al fine di conseguire, sia a livello regionale che a livello nazionale, l'omogeneità dei nuovi servizi telematici, lo scambio di soluzioni, risorse e buone pratiche e l'ottenimento di economie di scala;
- monitorare dello stato di avanzamento del progetto, l'efficacia e l'efficienza della Rete e dei servizi in rete ed a darne informazione alla Presidenza;
- istruire le procedure di gara per l'acquisizione dei beni e servizi necessari per lo sviluppo ed il funzionamento della Rete;
- promuovere lo sviluppo di nuovi servizi telematici in favore dei cittadini e delle imprese e per migliorare il funzionamento delle amministrazioni pubbliche.

Per gli aspetti di natura più strettamente tecnico-informatica, l'Ufficio di Presidenza si avvale del Centro Tecnico.

A.4.2 Il Centro Tecnico della RUPAR

Il **Centro Tecnico** svolge le attività tecniche necessarie per la progettazione, il coordinamento, l'operatività ed il controllo della RUPAR ed è responsabile della qualità delle soluzioni tecniche adottate e dei servizi erogati.

Tra le attività del Centro Tecnico rientrano:

- il disegno iniziale della RUPAR e delle sue successive evoluzioni;
- la definizione e la diffusione alle Amministrazioni locali ed ai fornitori di servizi telematici di procedure, schemi, livelli di qualità dei servizi richiesti e direttive tecniche necessarie per garantire l'unitarietà e la omogeneità della Rete, elevate prestazioni, costi contenuti e sicurezza;
- l'assistenza alla Regione nella qualificazione dei fornitori di servizi telematici della RUPAR;
- l'assistenza tecnica e contrattuale alle Amministrazioni Locali ed ai fornitori per la progettazione e la realizzazione delle parti di loro competenza e per lo sviluppo di nuovi servizi telematici che richiedono il concorso di più enti;

- l’infrastrutturazione iniziale e la gestione degli apparati e dei servizi generali necessari per il funzionamento dei nodi di interconnessione delle reti dei fornitori;
- il controllo sulla qualità dei servizi erogati dai fornitori e la validazione della compatibilità delle nuove applicazioni rispetto alle specifiche della RUPAR;
- la supervisione della gestione della sicurezza della RUPAR;
- il coordinamento dei fornitori per la risoluzione di problemi e la realizzazione di miglioramenti;
- i rapporti tecnici con il Centro Tecnico della Rete Nazionale;
- il controllo sui costi e sulla qualità complessiva delle prestazioni e della RUPAR;
- l’individuazione e la proposizione di interventi volti al superamento di eventuali problemi rilevati ed al miglioramento delle prestazioni esistenti;
- la predisposizione di rapporti informativi per consentire all’Ufficio di Presidenza della Regione di svolgere la sua funzione di sorveglianza;
- la definizione, l’attivazione e la gestione di Servizi di Cooperazione Applicativa.

A.4.3 Le Amministrazioni

Nella RUPAR le **Amministrazioni Locali** svolgono un duplice ruolo: quello di realizzatori di una parte della RUPAR e quello di utenti dei servizi della Rete.

In qualità di realizzatori le Amministrazioni locali acquisiscono autonomamente i servizi della RUPAR, individuano i servizi e le applicazioni da mettere in rete, promuovono lo sviluppo di nuovi servizi telematici. Come utenti fruiscono di tutti i servizi di base della Rete e dei servizi applicativi resi disponibili in Rete dalle altre Amministrazioni.

Sul piano finanziario usufruiscono dei servizi della RUPAR senza alcun costo per cinque anni, ad esclusione dei costi per i servizi aggiuntivi che potranno acquisire autonomamente dai fornitori.

Le Amministrazioni aderiscono al progetto semplicemente con l'acquisizione dei servizi RUPAR tramite le normali procedure di acquisizione di beni e servizi previste dalla legge nel caso di restrizione preventiva ad un insieme di possibili fornitori (albo dei fornitori certificati dal Centro Tecnico della RUPAR).
Ciascuna Amministrazione può richiedere ulteriori servizi e/o servizi di qualità superiore a quelli previsti dalla RUPAR accollandosi i maggiori costi.

Le singole Amministrazioni provvederanno autonomamente all'espletamento delle procedure di affidamento ed alla contrattualizzazione. E' previsto che il Fornitore emetta fatture per l'intero ammontare dei servizi, di base ed opzionali, dopo aver scontata la propria parte di cofinanziamento, direttamente verso l'Amministrazione che, a sua volta, chiederà alla Regione Puglia la copertura finanziaria degli importi di sua pertinenza (quota di cofinanziamento pubblico). La durata dei singoli contratti sarà di un anno rinnovabile secondo le vigenti procedure di legge.

Schemi tipo dei **contratti** saranno resi disponibili dal Centro Tecnico anche sul proprio Portale web (**http://ct.rupar.puglia.it**).

Con l'adesione al progetto la singola Amministrazione assume semplicemente l'impegno a partecipare fattivamente alla RUPAR ed ad attenersi alle procedure ed alle regole concordate con l'Ufficio di Presidenza della Giunta Regionale ed il Centro Tecnico. E' richiesto anche il rispetto di alcuni semplici vincoli, quello di collegarsi alla RUPAR mediante i servizi di un unico fornitore di servizi, di non dotarsi di ulteriori collegamenti a Internet e di istituire, nel caso in cui non esistesse già, un Servizio Informatico interno per la gestione dei rapporti con il fornitore e con il Centro Tecnico della RUPAR

Tramite il Servizio Informatico le Amministrazioni potranno rivolgersi per qualsiasi questione tecnica al Centro Tecnico della RUPAR, anche ad esempio per avere delle linee guida circa la progettazione e la realizzazione delle loro reti interne.

A.4.4 I fornitori di servizi di trasporto e di interoperabilità di base

I **Fornitori dei Servizi RUPAR** (**FSR**) hanno la responsabilità di realizzare l'interconnessione della singola Amministrazione alla RUPAR (fornendo il Servizio di Trasporto) e anche i servizi di interoperabilità applicativa e di interoperabilità tecnica; essi sono responsabili della attuazione delle misure di sicurezza dal lato della singola Amministrazione cliente.

I FSR provvedono anche all'erogazione alle singole Amministrazioni dei cosiddetti servizi di supporto che comprendono l'assistenza all'utenza finale (help desk), la gestione della integrità dei dati, il monitoraggio dei servizi, la registrazione e l'archiviazione delle attività svolte sulla rete.

L'ammissione alle procedure che ciascuna Amministrazione indirà per l'acquisto dei servizi è subordinata alla qualificazione come Fornitore della RUPAR.

Le imprese, infatti, devono superare la procedura di qualificazione che sarà attivata dalla Regione Puglia mediante una gara di evidenza pubblica, in quel contesto esse dovranno presentare le loro offerte di servizi. Le offerte rispondenti ai requisiti tecnici e compatibili con i costi della RUPAR sono inserite nel repertorio delle offerte usufruibili da parte delle Amministrazioni.

I fornitori possono offrire alle singole Amministrazioni anche servizi aggiuntivi rispetto a quelli previsti dalla RUPAR.

Le aziende ammesse sono tenute a comunicare al Centro Tecnico anche le loro offerte di riferimento per servizi aggiuntivi, in modo da consentire al Centro di assolvere il proprio servizio di assistenza nei confronti delle Amministrazioni.

Le aziende selezionate rispondono contrattualmente dei propri servizi alla Amministrazione appaltante ed alla Regione Puglia per tramite del Servizio Informatico interno della Amministrazione e del Centro Tecnico della RUPAR e sono tenute:

- ad erogare i servizi in conformità con gli standard tecnici definiti dal Centro Tecnico tramite appositi Centri di gestione, attivi 365 giorni l'anno, 24 ore al giorno, contattabili tramite numero verde telefonico, un numero verde di fax ed un indirizzo di posta elettronica
- a monitorare costantemente i servizi erogati
- ad assicurare la massima collaborazione al Centro Tecnico ed agli altri Centri di Gestione per la soluzione di problemi e miglioramenti delle prestazioni della Rete.

La collaborazione con il Centro Tecnico si estende alle attività di rilevazione di segnalazioni e problemi posti dagli utenti finali e di monitoraggio dei servizi di interoperabilità.

L'attività dei fornitori è oggetto di controlli non preannunciati da parte del Centro Tecnico per la verifica degli adempimenti e dei livelli di servizio contrattualmente definiti.

A.4.5 I fornitori di servizi di applicativi

I **fornitori di servizi applicativi** gestiscono e rendono fruibili alle Amministrazioni ed agli utenti finali le applicazioni telematiche della RUPAR.

Si tratta di procedure informatiche, banche dati, portali web, servizi on line che le Amministrazioni realizzano avvalendosi di queste aziende per la realizzazione e la gestione di servizi integrati ai cittadini ed alle imprese.

Gran parte di queste applicazioni saranno avviate da ogni singola Amministrazione in modo autonomo secondo la propria visione e la propria strategia. Altre dalla Regione o da gruppi di Amministrazioni per finalità comuni o per attività e servizi che richiedono il concorso di più Amministrazioni.

La Misura 6.3 del POR Puglia 2000-2006 prevede e finanzia tre di queste applicazioni basate sulla cooperazione interamministrativa:

- il **Sistema** di **Interscambio** tra **Catasto** e **Comuni** per la gestione integrata delle informazioni catastali e territoriali
- il **Sistema Sanitario Regionale**, per la gestione integrata delle informazioni e delle procedure del Sistema Sanitario Regionale e l'integrazione tra l'anagrafe sanitaria e quella comunale
- l'**Osservatorio** della **Finanza Locale** per la raccolta, l'elaborazione e la diffusione dei dati sulla destinazione della spesa del sistema delle autonomie locali pugliesi

Altre applicazioni saranno realizzate nell'ambito di specifiche Misure del POR o con ulteriori iniziative promosse dalla Regione, da Amministrazioni locali o da privati.
I fornitori di servizi applicativi possono al riguardo svolgere una o più delle seguenti funzioni:

- progettazione e realizzazione delle applicazioni telematiche della RUPAR,
- conduzione operativa e sistemistica,
- manutenzione correttiva ed evolutiva,
- assistenza tecnica ed assistenza agli utenti finali.

L'Amministrazione Regionale intende favorire lo sviluppo di modalità coerenti e omogenee di cooperazione tra le applicazioni che saranno progressivamente attivate sulla Rete Regionale dalle Amministrazioni locali attraverso i propri fornitori di servizi applicativi.

Allo scopo il Centro Tecnico definirà protocolli, linee guida, raccomandazioni e standard da seguire e metterà a disposizione delle Amministrazioni servizi informatici (a partire da quelli di cui alla successiva sezione A.4.6) che ne agevolino l'adozione.

Le Amministrazioni collegate alla Rete Regionale dovranno impegnare in sede contrattuale i fornitori al rispetto dei protocolli e degli standard tecnici definiti dal Centro Tecnico ed a collaborare con lo stesso per garantire la piena e corretta integrazione delle proprie applicazioni nella RUPAR, nonché per raccogliere le informazioni sul livello di utilizzo e soddisfazione degli utenti.

Le Amministrazioni che impegnino in tal senso i propri fornitori potranno richiedere l'assistenza del Centro Tecnico per quanto riguarda la corretta impostazione e la risoluzione delle problematiche di cooperazione applicativa sia in sede istruttoria che in sede concorsuale che, infine, in sede di collaudo delle applicazioni RUPAR.

Analogamente a quanto previsto per i servizi di trasporto e di interoperabilità, i Servizi di cooperazione applicativa su RUPAR saranno sottoposti a controlli da parte del Centro Tecnico per la verifica della correttezza dell'inserimento e dell'operatività nel contesto RUPAR.

A.4.6 I servizi di supporto alla cooperazione

La gestione dei servizi di supporto alla cooperazione applicativa è una funzione del Centro Tecnico che provvede specificamente allo sviluppo ed alla erogazione dei servizi di base per le applicazioni RUPAR.

Questi servizi rendono possibile l'integrazione delle applicazioni, tipicamente non omogenee e proprietarie, in un contesto di elevata complessità per la presenza di più Amministrazioni e più aziende.

Si basano sulla architettura cooperativa della RUPAR che garantisce:

- trasparenza funzionale della RUPAR rispetto alle applicazioni;
- trasparenza delle applicazioni rispetto alla organizzazione ed alle risorse della RUPAR;
- il rispetto del principio di non intrusione secondo il quale non devono essere richiesti condizionamenti o modifiche delle applicazioni.

I servizi di base per la cooperazione applicativa che saranno forniti dal Centro Tecnico includono:

- informazioni ed assistenza tecnica alle Amministrazioni ed ai fornitori di servizi applicativi per lo sviluppo e la messa in rete di applicazioni conformi alla RUPAR;
- l~~L~~a pubblicazione sul Portale web della RUPAR di tutte le informazioni sulle applicazioni disponibili nella Rete regionale;
- la gestione dei servizi di base per l'integrazione trasparente tra le applicazioni e la loro esposizione sulla Rete, la *directory* dei servizi ed il sistema di propagazione degli eventi di cooperazione amministrativa, illustrati in maggior dettaglio nel par. C.1.2.

Ulteriori servizi di sostegno allo sviluppo e gestione di applicazioni di cooperazione amministrativa sulla Rete Regionale

saranno progressivamente organizzati e resi disponibili nell'ambito del mandato istituzionalmente conferito al Centro Tecnico.

Questi aspetti sono affrontati attraverso la predisposizione di idonee procedure organizzative e strumentazioni.

Per l'integrità, la provenienza, l'autenticità e la privacy, i servizi in oggetto fanno riferimento al sistema di crittografia a chiave pubblica che è alla base della firma digitale ammessa dalla normativa vigente per la sottoscrizione dei documenti informatici

I fornitori del servizio di certificazione saranno scelti tra le aziende accreditate come *Certification Authority* dall'AIPA, che provvederanno alla distribuzione delle firme digitali agli utenti finali della RUPAR (Amministratori, Dirigenti pubblici, impiegati, ecc.), nonché ad assistere tecnicamente le Amministrazioni nell'utilizzo della firma e dei certificati digitali.

A.5 Quadro normativo

A.5.1 Leggi e Regolamenti pertinenti

Il novero di provvedimenti che regola lo sviluppo ed il funzionamento delle reti e dei servizi telematici è diventato sempre più ricco e corposo dal primo provvedimento preso il 5 settembre 1995 dalla Presidenza del Consiglio dei Ministri riguardo la Rete Unitaria della Pubblica Amministrazione.

La forte spinta all'innovazione delle amministrazioni pubbliche e la rapida evoluzione delle tecnologie fanno pensare altresì ad ulteriori interventi normativi nel prossimo futuro.

Per agevolare la comprensione del quadro normativo appare utile classificare direttive, leggi, decreti, raccomandazioni e standard in disposizioni che regolano:

- La RUPA ed il Centro Tecnico della RUPA
- Il ruolo delle Regioni e degli Enti Locali nella RUPA
- I servizi di telecomunicazione
- La validità giuridica dei documenti informatici e la firma digitale
- La sicurezza dei sistemi informatici e telematici
- Gli appalti di beni e servizi informatici

Quadro normativo relativo alla RUPA ed al Centro Tecnico

Il progetto intersettoriale per la RUPA è proposto per la prima volta dall'AIPA nel Piano di Informatizzazione della Pubblica Amministrazione per il triennio 1995-1997.

La Presidenza del Consiglio dei Ministri con la Direttiva del 5 settembre 1995 fissa finalità ed organizzazione della Rete, ruoli e responsabilità del progetto.

L'iniziativa, considerata prioritaria per gli obiettivi di efficienza, miglioramento dei servizi, potenziamento dei supporti conoscitivi e contenimento dei costi dell'azione amministrativa individuati dal decreto legislativo 12 febbraio 1993, n. 39, ha come finalità:

L'interconnessione telematica delle reti delle singole amministrazioni pubbliche.
L'accesso da parte del sistema informativo di ciascuna amministrazione ai dati e alle procedure residenti nei sistemi informativi delle altre, nel rispetto della normativa in materia di limiti all'accesso, di segreto e di tutela della riservatezza (con predisposizione, anche in sede tecnica).

Lo scambio di ogni documento ed informazione utile per le attività interne delle Amministrazioni e per l'erogazione unificata di dati e prestazioni amministrative ai cittadini.

Le reti delle singole amministrazioni, anche dopo l'integrazione all'interno della RUPA, restano sotto la responsabilità di queste ultime, conservandosi a ognuna di esse anche la competenza e responsabilità della progettazione e realizzazione dei propri sistemi informativi, pur se nel rispetto di nuove regole tecniche comuni.

Il Governo s'impegna ad adottare le misure legislative, regolamentari ed amministrative per dare compiuta effettività alla RUPA.

La Presidenza del Consiglio dei Ministri svolge le funzioni di indirizzo e di vigilanza sull'intera realizzazione del progetto della Rete unitaria.

All'AIPA è affidato il compito di definire le regole tecniche per la interoperabilità tra le reti delle singole amministrazioni e lo sviluppo di servizi telematici comuni.

Alla Funzione pubblica quello di adottare iniziative rivolte a promuovere interventi organizzativi e procedurali (anche ai fini della semplificazione) correlati alla realizzazione della nuova Rete ed - in collaborazione con l'Autorità per l'informatica e avvalendosi della Scuola Superiore della P.A. attività di formazione volte a

sviluppare l'approccio informatico allo svolgimento del lavoro amministrativo.
Alle singole Amministrazioni è richiesto di adeguare organizzazione e procedure in modo da renderle coerenti con il nuovo assetto integrato dei sistemi informativi della pubblica amministrazione.

Lo studio di fattibilità della RUPA, AIPA gennaio 1996, disponibile su www.aipa.it, fornisce la soluzione architetturale. Nello studio sono affrontate anche le tematiche della sicurezza, della acquisizione dei servizi di telecomunicazione e del ruolo degli Enti Locali.

In estrema sintesi stabilisce che:

L'obiettivo più immediato della Rete unitaria è una struttura tecnologica atta a garantire, agli utenti abilitati, il dialogo tra loro in condizioni di elevata sicurezza, mediante accesso ai dati e alle procedure contenuti nei sistemi informativi automatizzati della propria e di altre amministrazioni, indipendentemente dalle reti attraversate e dalle tecnologie adottate dai singoli sistemi informativi, nel rispetto dell'autonomia di ogni singola amministrazione.

La RUPA più che una infrastruttura fisica è una infrastruttura di servizi. I servizi erogati sono quelli di trasporto, di interoperabilità e di cooperazione.

I servizi di trasporto riguardano sia i collegamenti geografici interni a ciascuna amministrazione, sia quelli diretti tra le amministrazioni, eventualmente già esistenti.

I servizi di interoperabilità riguardano funzioni di adattamento e conversione per lo scambio di informazioni tra sistemi, reti e applicazioni, tra loro anche non omogenee. Rientrano tra questi la posta elettronica, il trasferimento file, il terminale virtuale, il collegamento ad Internet, erogati per il tramite di un Centro di gestione, realizzato ad hoc. Sono corredati di un sistema di monitoraggio della qualità, di help-desk specialistico, di servizi di formazione degli utenti, di supporto tecnico alle amministrazioni. I servizi di cooperazione consentono, invece, alle applicazioni informatiche di un'amministrazione di fare uso dei servizi applicativi messi a disposizione da altre amministrazioni.

Gli Utenti della RUPA sono le Amministrazioni pubbliche centrali e gli Enti pubblici non economici nazionali. Per questi organismi, è obbligatorio avvalersi dei servizi di trasporto e di interoperabilità della RUPA attraverso la sottoscrizione di appositi contratti di fornitura con i fornitori aggiudicatari dei rispettivi appalti. Le amministrazioni locali fruiscono della facoltà di avvalersi dei medesimi servizi.

Allo studio segue il 25 febbraio 1997, sempre a cura dell'AIPA, il documento sulla Architettura Applicativa, anch'esso consultabile sul sito www.aipa.it.

La Legge 15 maggio 1997, n. 127 istituisce presso l'AIPA un Centro Tecnico, operante con autonomia amministrativa e funzionale, sotto la direzione e il controllo dell'Autorità, per l'assistenza ai soggetti che utilizzano la Rete unitaria della pubblica amministrazione.

L'organizzazione ed il funzionamento del Centro Tecnico della RUPA sono disciplinati dal Decreto del Presidente della Repubblica 23 dicembre 1997, n. 522.

Al Centro Tecnico sono assegnati compiti di coordinamento e vigilanza delle attività del fornitore dei servizi di trasporto e del fornitore del servizio di interoperabilità, di promozione e di controllo di idonee misure di sicurezza, di pianificazione dell'evoluzione tecnica della Rete e di assistenza alle amministrazioni sotto il profilo tecnico e della cooperazione applicativa.

Il 5 febbraio 1998 il Centro Tecnico pubblica due bandi di gara, uno per il servizio di trasporto, l'altro per i servizi di interoperabilità. Le due gare sono aggiudicate rispettivamente alla società Telecom Italia il 28 dicembre 1998 ed alla società EDS l'11 febbraio 1999.

Ognuno degli Aggiudicatari della gara ha costituito per contratto un'apposita Società avente come oggetto sociale esclusivo la fornitura dei servizi oggetto della gara e soggette a vincoli nei confronti del Centro Tecnico, ad esempio la preventiva approvazione dello Statuto. La società costituita da Telecom Italia si chiama Pathnet. La società costituita da EDS Italia si chiama EDS P.A.

Le amministrazioni stipulano due contratti di fornitura, uno con la Società costituita dall'Aggiudicatario dei Servizi trasmissivi di Trasporto e l'altro con la Società costituita dall'Aggiudicatario dei Servizi per l'Interoperabilità.

I contratti di fornitura hanno le stesse scadenze dei contratti quadro, cinque anni con possibilità di rinnovo di anno in anno fino ad un massimo di quattro.

I prezzi unitari dei servizi riportati nel contratto quadro valgono per tutte le amministrazioni e sono oggetto di una revisione generale annuale in relazione all'andamento del mercato. Ogni amministrazione paga i servizi di trasporto in base alle tipologie di servizi attivati presso i propri punti di accesso, applicando mensilmente i prezzi unitari validi alla data. I corrispettivi vengono adeguati mensilmente in relazione al tipo ed al numero di punti di accesso utilizzati.

Per quanto riguarda i servizi di interoperabilità, per i primi tre anni il prezzo annuo viene suddiviso in rate mensili:

- il 40% (Canone di accesso) viene ripartito in uguale misura tra le amministrazioni;
- il 60% (Canone di gestione) a carico del Centro Tecnico.

Dal quarto anno il Canone mensile di accesso della singola amministrazione resta invariato e il Canone mensile di gestione è sostituito da un costo mensile del traffico, a carico della singola amministrazione, calcolato in base ai "messaggi" scambiati/utilizzati nel mese.

Il Fornitore dei servizi di trasporto ha realizzato un Centro di Gestione del Trasporto (CG-T), responsabile dell'erogazione dei servizi di trasporto. Il Fornitore dei servizi di interoperabilità ha realizzato un Centro di Gestione per l'Interoperabilità (CG-I), responsabile della gestione dei servizi che riguardano la Rete unitaria. Entrambi i Centri operano sotto il controllo del Centro Tecnico.

Ogni amministrazione è tenuta ad avvalersi di una propria struttura gestionale chiamato Centro di Gestione dell'amministrazione (CG-Amm). i cui principali compiti sono di:

Interfaccia del Centro di Gestione per il Trasporto e del Centro di Gestione per l'Interoperabilità.

Supervisione del funzionamento della rete geografica dell'amministrazione.
Help-desk di primo livello per tutti i posti di lavoro delle Amministrazioni

Per acquisire i Servizi base di trasporto e di interoperabilità le amministrazioni non devono effettuare gare e non devono richiedere il parere di congruità tecnico-economica all'Autorità.

Per acquisire i Servizi addizionali per l'interoperabilità previsti nel contratto quadro non devono effettuare gare, né richiedere il parere di congruità all'AIPA, se acquistati dall'aggiudicatario della gara per i servizi di interoperabilità della RUPA.

Il Piano di azione di e_Government della Funzione Pubblica del giugno 2000 inserisce la RUPA all'interno della Rete Nazionale della Pubblica Amministrazione. L'obiettivo del Piano è la connettività di tutte le amministrazioni e gli enti locali utilizzando come base la rete e la tecnologia Internet.

La Legge n. 340 del 24 novembre 2000 posiziona Il Centro Tecnico come organismo autonomo collocato nell'ambito della Presidenza del Consiglio dei Ministri.

Il Centro Tecnico, pur mantenendo i precedenti compiti e responsabilità, assume il coordinamento e l'attuazione dei progetti del Piano di e_Government, tra cui il progetto per la Rete Nazionale che ingloba la RUPA.

Quadro normativo relativo al ruolo delle Regioni e degli Enti Locali nella RUPA

Lo studio di fattibilità dell'AIPA del 1996 prevede che nella Rete unitaria gli Enti Locali svolgano un ruolo fondamentale sia come fornitori di informazioni e servizi necessari per la cooperazione tra sistemi applicativi delle amministrazioni centrali, sia come attori di processi di cooperazione che coinvolgono sistemi applicativi delle amministrazioni centrali e locali, sia, soprattutto, come erogatori di servizi finali verso i cittadini.

La RUPA, consente alle amministrazioni locali, in particolare ai Comuni, di proporsi come sportello dell'intera Pubblica Amministrazione che, tramite la rete, può presentarsi all'utente finale come un sistema unitario di servizi. Inoltre agevola il processo di decentramento in atto delle funzioni amministrative senza diminuire o rendere più costosa l'efficienza delle organizzazioni.

Lo studio prevede che le amministrazioni locali non siano obbligate come le amministrazioni centrali a collegarsi alla RUPA ma che possano usufruire delle stesse modalità nel caso di adesione.

Il Decreto legislativo 28 agosto 1997, n. 281, inserisce tra le attribuzioni della Conferenza Stato-regioni, quella concernente l'interscambio di dati ed informazioni e la costituzione di banche dati sulle rispettive attività, accessibili sia dallo Stato che dalle regioni e dalle province autonome. Le norme tecniche ed i criteri di sicurezza per l'accesso ai dati ed alle informazioni sono stabiliti di intesa con l'AIPA.

Il 12 settembre 1995 è stato sottoscritto un protocollo di intesa, ai sensi dell'art. 7 comma 2 del d.lgs. 12 febbraio 1993, n. 39, tra il Presidente del Consiglio dei Ministri, l'AIPA, proponente, e la Conferenza Stato-Regioni, finalizzato alla collaborazione in materia di pianificazione degli investimenti, di linee di normalizzazione e criteri di progettazione di sistemi informativi, in cui si prevedono attività di sperimentazione sia sul piano delle architetture tecnologiche, sia per quanto riguarda i servizi telematici di interoperabilità e cooperazione tra i sistemi informativi dei vari livelli di governo della Pubblica Amministrazione.

La Conferenza Stato-Regioni, nella seduta del 25 settembre 1997, ha sancito l'accordo tra Governo, Regioni e AIPA, avente ad oggetto "Lo sviluppo delle Reti telematiche a livello regionale e la Rete Unitaria delle Pubbliche Amministrazioni" e le relative linee di indirizzo, in base al quale viene qualificato obiettivo stra-

tegico di rilevanza nazionale lo sviluppo di reti unitarie a livello regionale e la loro interconnessione con la RUPA.

In attuazione dell'accordo, le Regioni propongono all'AIPA la stipula di convenzioni per la progettazione e la sperimentazione delle reti unitarie delle pubbliche amministrazioni a livello regionale (RUPAR), e l'interconnessione di queste con la RUPA e di progetti comuni relativi all'erogazione di servizi mediante l'integrazione dei flussi informativi tra la Pubblica Amministrazione centrale e quella locale.

Per indirizzare e programmare le attività previste nelle convenzioni, per ognuna è costituito un Comitato tecnico-scientifico, composto da quattro membri, due nominati dalla Regione e due dall'Autorità.

Hanno firmato convenzioni con l'AIPA le Regioni Piemonte (1998), Toscana (1998), Lombardia (1998), Marche (1998), Puglia (1999), Sicilia (1999), Emilia-Romagna (1999), Friuli Venezia Giulia (1999), Abruzzo (2000), Basilicata (2000).

Il Piano di azione di e-Government della Funzione Pubblica del giugno 2000 conferma il ruolo primario alle singole Regioni nella realizzazione delle infrastrutture e dei servizi telematici per l'e_Government e per l'interconnessione e l'interoperabilità dei sistemi informativi tra le Regioni e tra queste e le Amministrazioni centrali.

Il Piano assegna agli enti locali, in particolare ai comuni, il ruolo di realizzatori e gestori degli sportelli telematici di front-office per la erogazione dei servizi integrati al cittadino ed alle imprese.

Il documento approvato dall'AIPA il 12 ottobre 2000, Connessione delle Pubbliche Amministrazioni Locali alla Rete Unitaria, riassume alcuni principi fondamentali posti alla base della progettazione della Rete Unitaria e di discutere se e come questi principi risultino tuttora validi nell'indirizzare la realizzazione dei possibili servizi applicativi da parte delle Amministrazioni Centrali e Locali.

Il documento apre agli Internet service provider in grado di garantire il collegamento alla Rete Unitaria a livello di indirizzamento IP e di fornire livelli di servizio confrontabili con quelli degli strati di interoperabilità e di cooperazione.

Questi provider, referenziati come "RUPA service provider", avranno una propria certificazione (con modalità e tempi da stabilire in seguito ad opportuni accordi tra le parti) e potranno far parte di una lista certificata a cui un qualsiasi utente potrà rivolgersi per ottenere i servizi applicativi predisposti dalle amministrazioni con livelli di servizio adeguati ai requisiti delle applicazioni coinvolte.

Quadro normativo per i servizi di telecomunicazione

Il quadro normativo che regola il mercato dei servizi pubblici di telecomunicazioni è essenzialmente quello definito dal D.L.vo 17 marzo 1995, n. 103, "Recepimento della Direttiva 90/388/CEE relativa alla concorrenza nei mercati dei servizi di telecomunicazioni", e dal DPR 4 settembre 1995, n. 420, "Regolamento recante determinazione delle caratteristiche e delle modalità di svolgimento dei servizi di telecomunicazioni di cui all'art.2, comma 1 del Decreto Legislativo 17 marzo 1995 n. 103".

Questi provvedimenti concludono l'iter di recepimento nella legislazione italiana di una serie di Direttive CEE, prime tra tutte la direttiva 90/387 del Consiglio CEE relativa all'istituzione del mercato interno dei servizi di telecomunicazione mediante la realizzazione della fornitura di una rete aperta di telecomunicazioni (Open Network Provision - ONP), la direttiva 90/388/CEE relativa alla concorrenza nei mercati dei servizi di telecomunicazione e la direttiva 92/44/CEE, sulla applicazione di una fornitura di rete aperta alle linee affittate.

Tali atti normativi hanno determinato la liberalizzazione della prestazione di quasi tutti i servizi di telecomunicazione, compresi quelli vocali, per gruppi chiusi di utenti, purché essi siano offerti utilizzando esclusivamente i collegamenti commutati o diretti della rete pubblica.

Tutti i servizi di interesse della Rete unitaria possono essere offerti da una pluralità di soggetti, in particolare almeno da tutti gli operatori autorizzati a offrire al pubblico i servizi liberalizzati e iscritti quindi nell'apposito Pubblico registro istituito presso il Ministero delle poste e delle telecomunicazioni (art. 8 del DPR 420/95).

Per la RUPAR i principali standard tecnici da seguire sono quelli prescritti dal regolamento tecnico approvato dal Ministero delle Poste e delle Telecomunicazioni, gli standard dell'IETF per il TCP/IP e, per le tecnologie di trasmissione, gli standard emessi da:

- IEEE (Institute of Electrical and Electronics Engineers, URL: http://www.ieee.org) normalmente recepiti dall'ISO (International Standard Organization, URL: http://www.iso.ch)
- ETSI (European Telecommunication Standard Institute, URL: http://www.etsi.org)
- ITU-T (International Telecommunication Union-Telecom, URL: http://www.itu.int/ITU-T/)

- ATMForum (URL: http://www.atmforum.com)
- FrameRelayForum (URL: http://www.frforum.com)

Quadro normativo relativo alla validità giuridica dei documenti informatici ed alla firma digitale

Le disposizioni che riconoscono la validità dei documenti prodotti con strumenti informatici ha spalancato la strada all'effettivo impiego dei servizi telematici nella Pubblica Amministrazione.

La maggior parte di queste disposizioni sono contenute nel Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

La legge riconosce la validità giuridica del validità e la rilevanza a tutti gli effetti di legge del documento informatico da chiunque formato, la conservazione su supporto informatico e la trasmissione con strumenti telematici, se conformi alle disposizioni del testo unico. Sono altrettanto validi e rilevanti i moduli ed i formulari elettronici resi disponibili per via telematica dalle pubbliche amministrazioni.

Il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche definite soddisfa il requisito legale della forma scritta e ha efficacia probatoria. Gli stessi contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale sono validi e rilevanti a tutti

gli effetti di legge. Nella Pubblica Amministrazione l'apposizione della firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. E' il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura, deve munirsi di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione, mediante la quale il soggetto pubblico o privato che effettua la certificazione (certficatore) garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, identifica quest'ultimo e attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni.

Le attività di certificazione sono effettuate da certificatori che rispondono ai requisiti posti dalla legge, inclusi in un apposito elenco pubblico predisposto tenuto e aggiornato dall'AIPA, consultabile anche per via telematica.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La trasmissione con modalità che assicurino l'avvenuta consegna equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge.

Al fine di tutelare la riservatezza dei dati personali sensibili, i certificati ed i documenti trasmessi da una pubblica amministrazione possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite.

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

Le regole tecniche per i documenti informatici sono definite con decreto del Presidente del Consiglio dei Ministri sentita l'Autorità per l'informatica nella pubblica amministrazione e sono adeguate alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche, con decorrenza almeno biennale. Con il medesimo decreto sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico anche con riferimento all'eventuale uso di chiavi biometriche.

Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono invece definite dall'Autorità per l'informatica nella pubblica amministrazione d'intesa con l'amministrazione degli archivi di Stato e, per il materiale classificato, con le Amministrazioni della difesa, dell'interno e delle finanze, rispettivamente competenti.

Il Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 stabilisce le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici

Il decreto fissa gli algoritmi di generazione e verifica delle firme digitali, gli algoritmi di generazione dell'impronta (hash), le caratteristiche generali e le modalità di generazione e conservazione delle chiavi asimettriche, il formato della firma digitale, gli strumenti e le procedure per la generazione e la verifica delle

firme, il formato dei certificati e le modalità di accesso al registro dei certificati, le regole tecniche per la certificazione delle chiavi, per la validazione temporale e per la protezione dei documenti informatici e per le pubbliche amministrazioni

Quadro normativo in materia di Sicurezza dei sistemi informatici e telematici

Il tema della sicurezza della RUPA è affrontato dallo studio di fattibilità della RUPA, AIPA gennaio 1996 e nei documenti relativi alla architettura della Rete, tutti disponibili sui siti www.aipa.it e www.ct.rupa.it.

Tutti gli aspetti relativi alla sicurezza della RUPA sono supervisionati dal Centro tecnico.

Nella RUPA è garantita la trasparenza della gestione dei flussi di dati dal punto di vista del trasporto, in quanto il Centro di gestione di trasporto non è inserito nei flussi. In pratica le informazioni non transitano per il Centro, ma questo serve solo per la supervisione e il controllo degli apparati e dei sistemi che sono preposti ai servizi di trasporto.

Vi sono garanzie di riservatezza, ottenute traverso altri servizi che garantiscono la comunicazione protetta tra Amministrazioni, la protezione del nome del mittente e del destinatario e dei contenuti della comunicazione, la correttezza ed il corretto inoltro delle informazioni che vengono gestite dal Centro di gestione di interoperabilità.

I centri sono situati in edifici e locali protetti, sottoposti a controlli, dotati di protezioni per gli accessi ai sistemi.

Gli operatori sono sottoposti a identificazione e autenticazione. Esistono profili differenziati, non tutti possono fare le stesse cose.

Tutte le azioni effettuate sui sistemi sono sistematicamente rilevate e controllate e le componenti critiche sono protette da sistemi di autenticazione forte basati su password.

Sulle porte di accesso delle amministrazioni vi sono ulteriori protezioni e tutto il traffico della posta elettronica tra le amministrazioni e tra queste mondo Internet è soggetto a protezione antivirus.

Il Centro tecnico e le amministrazioni svolgono periodicamente test di impenetrabilità e verifiche periodiche dei livelli di sicurezza.

L'AIPA ha anche pubblicato nell'ottobre 1999 un documento "Linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati nella Pubblica Amministrazione" con l'intento di sensibilizzare le Amministrazioni sul tema Scurezza e indirizzarle per la realizzazione di idonee misure a salvaguardia dei sistemi e dei servizi informatici di loro competenza.

Ulteriori indicazioni sull'argomento sono state fornite dall'AIPA con la raccomandazione in materia di sicurezza dei siti Internet, consultabile sul sito dell'AIPA. Il documento è articolato in quattro parti, che riguardano, rispettivamente: la procedura organizzativa ed amministrativa, la procedura di monitoraggio, la procedura di intervento e ripristino, la procedura di certificazione.

Strettamente collegati con i temi della sicurezza sono le disposizioni inerenti:

- La tutela del diritto di autore, Legge 22 aprile 1941 n. 633, Integrata dal D.Lgs. 29 dicembre 1992 n. 518 e dal D.Lgs. 6 maggio 1999 n. 169
- La tutela giuridica delle banche dati, Decreto legislativo 6 maggio 1999, n. 169 in attuazione della direttiva 96/9/CE
- Le modificazioni e le integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica, Legge 23 dicembre 1993 n. 547.

La legge in materia di criminalità informativa prevede diversi reati tra cui quelli di:

- danneggiamento, distruzione o alterazione fraudolenta del software;
- danneggiamento o distruzione di sistemi informatici di pubblica utilità;
- diffusione di programmi diretti a danneggiare o interrompere un sistema informatico;
- accesso non autorizzato ad un sistema informatico o telematico;
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- violazione della corrispondenza inviata per via telematica;
- falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche;
- falso in documenti informatici pubblici;
- frode informatica.

Quadro normativo sugli appalti pubblici di servizi e forniture

Le norme più rilevanti sono quelle contenute nel D.L.vo n. 157/95 di attuazione della direttiva 2/50/CEE in materia di appalti pubblici di servizi che definisce le procedure di aggiudicazione (c.d. gare comunitarie) di contratti tra amministrazioni aggiudicatrici e prestatori di servizi. Per le forniture di prodotti trova applicazione il D.L.vo n. 358/1992, di attuazione delle direttive 77/62/CEE, 80/767/CEE, 88/295/CEE.

Le forniture di beni e le connesse prestazioni di servizi in materia di sistemi informativi automatizzati sono disciplinate dal Decreto del Presidente del Consiglio 6 agosto 1997, n. 452. Il Decreto tratta della locazione e della locazione di apparecchiature informatiche e della licenza d'uso dei programmi.

Utile è anche la circolare pubblicata dall'AIPA, consultabile su www.aipa.it, per l'utilizzo della certificazione EN ISO 9000 in sede di gara. Con la Circolare l'AIPA intende aiutare le Amministrazioni a non confondere la certificazione di prodotto con la certificazione di processo (o il sistema qualità) ed ad evitare:

- di utilizzare i requisiti contrattuali inerenti alla certificazione non verificabili o difficilmente verificabili in sede di gara;
- richieste di certificazione relative a norme non compatibili con i servizi contrattualmente richiesti;

- l’uso della certificazione per la valutazione della capacità tecnica del fornitore;
- il generico riferimento alle norme EN ISO 9000 in sostituzione di precisi requisiti contrattuali relativi ai prodotti e servizi attesi, alle procedure da utilizzare, alle modalità di verifica dei livelli di servizio.

A.5.2 Individuazione delle responsabilità legali

Le attività correlate alla progettazione, allo sviluppo ed alla gestione della RUPAR fanno insorgere, tra i diversi soggetti che a vario titolo partecipano alla Rete, responsabilità ed obbligazioni che hanno rilevanza anche legale.

Sotto questo particolare aspetto di seguito sono prese in considerazione le relazioni tra:

- La Regione Puglia e l’Ue
- La Regione Puglia e le Amministrazioni
- I Fornitori e le Amministrazioni
- La Regione Puglia e il Centro Tecnico

La Regione Puglia risponde all'Ue delle azioni previste nella Misura 6.3 del POR Puglia analogamente a quanto avviene per le altre Misure che come è noto prevedono specifiche attività di sorveglianza, monitoraggio, valutazione e controllo ed interventi in caso di ritardi o inadempienze.

Verso le Amministrazioni locali della Puglia la Regione con la RUPAR si impegna realizzare ed a fornire una serie di servizi ed a coprire i costi di realizzazione del progetto e, per i primi cinque anni, i costi di funzionamento.

Gli Enti Locali che aderiscono alla RUPAR a loro volta si impegnano nei confronti della Regione a svolgere le attività loro delegate secondo le regole e le procedure definite.

Tutte le Amministrazioni, compresa la Regione Puglia, assumono reciprocamente l'impegno a collaborare per il pieno e corretto utilizzo della Rete e per la soluzione di eventuali problemi.

Le obbligazioni reciproche assunte dalla Regione Puglia e dagli Enti Locali possono essere classificate come volontarie, formali e obbligatorie.

Le prime nascono dalla libera iniziativa delle parti e non richiedono necessariamente un accordo (convenzione, patto, contatto, ecc.) scritto. Rientrano, ad esempio, in questa classe le obbligazioni assunte in fase di adesione delle singole Amministrazioni

alla RUPAR che ha luogo semplicemente acquisendo i servizi della RUPAR dai fornitori certificati dalla Regione.

Le obbligazioni formali richiedono necessariamente la stipula un accordo scritto (convenzione, patto, contatto, ecc.) tra le Amministrazioni nel quale sono specificamente indicati gli impegni delle parti e le misure da assumere in caso di inadempienze. Rientrano in questa classe le obbligazioni assunte dalla Regione nei confronti delle Amministrazioni per il pagamento dei servizi RUPAR utilizzati e quelli relativi allo sviluppo di specifici servizi di cooperazione applicativa.

Le obbligazioni obbligatorie derivano dall'applicazione di leggi ed anch'esse, come nel caso delle obbligazioni formali, richiedono la stipula di accordi scritti nei quali sono richiamate specificamente la legge da attuare.

Le aziende che forniscono i servizi per lo sviluppo ed il funzionamento della RUPAR assumono obblighi contrattuali in due specifichi momenti.

Nella fase di certificazione si impegnano direttamente, con la Regione ed indirettamente con tutte le altra Amministrazioni, a fornire beni e servizi a condizioni, livelli di servizio tempi e tariffe prestabiliti. Successivamente con la sottoscrizione dei contratti di forniture con le singole Amministrazioni, Regione inclusa, danno effettivo corso all'impegno precedentemente assunto in via generale.

Una particolare tipologia di fornitore è rappresentata dalla società che realizza e gestisce, per conto della Regione, il Centro Tecnico della RUPAR.

Tale società si impegna nei confronti della Regione, attraverso uno specifico contratto di servizio, a fornire una serie di servizi di carattere prevalentemente tecnico che riguardano la progettazione iniziale della Rete, il coordinamento delle attività delle Amministrazioni e dei fornitori, il controllo delle prestazioni e dei livelli di servizio erogati dai fornitori, l'evoluzione della Rete. Ne consegue che assume degli obblighi contrattuali direttamente nei confronti della Regione e, indirettamente, verso le Amministrazioni e stessi fornitori, evidentemente, in quest'ultimo caso, nell'interesse della Pubblica Amministrazione.

Normalmente le obbligazioni tra le Amministrazioni e tra queste ed i fornitori sono regolate da contratti nei quali sono specificamente specificati gli impegni reciproci, le modalità, i tempi ed i costi, le procedure e le penali per eventuali inadempienze, il foro competente per eventuali controversie legali.

I contraenti oltre al rispetto degli impegni esplicitamente indicati negli atti contrattuali sono tenuti delle norme del codice civile e del codice penale ed delle norme che regolano la materia oggetto del contratto, con particolare riferimento a quelle precedentemente indicate che riguardano i servizi di telecomunicazione, la validità giuridica dei documenti informatici, la privacy, il diritto d'autore e gli atti di criminalità informatica.

A.5.3 Criteri e normative per i diversi ruoli

Al di là degli obblighi rilevanti dal punto di vista strettamente legale a ciascuno dei soggetti protagonisti della RUPAR è richiesto il rispetto di linee di comportamento e regole generali per il successo del progetto ed il conseguimento degli obietti prefissati.

La Regione Puglia, che si è assunta il compito di promuovere e coordinare il progetto, si muove fondamentalmente secondo questi criteri:

- il rispetto delle raccomandazioni e dell'Ue in materia di gestione dei fondi comunitari e di sviluppo di infrastrutture telematiche per la Soceità dell'Informazione
- la partecipazione alle iniziative del Governo italiano in materia di Società dell'Informazione e di e_Government

- il coinvolgimento delle istituzioni e delle espressioni sociali, economiche e culturali pugliesi nei piani e nei progetti per lo sviluppo della Società dell'Informazione in Puglia
- la devoluzione agli Enti Locali, nel pieno rispetto della loro autonomia, di tutte le attività che possono essere loro assegnate per competenza amministrativa e capacità tecnica
- l'*outsourcing* a società informatiche e telematiche della realizzazione e gestione operativa e tecnica della RUPAR
- il monitoraggio sui risultati di progetto e l'eventuale pronta attivazione di interventi migliorativi e correttivi

Dalle singole Amministrazioni che partecipano alla Rete è atteso che:

- utilizzino la RUPAR per realizzare i propri programmi e delle proprie strategie di sviluppo
- siano disponibili collaborare con le altre Amministrazioni per lo sviluppo di servizi integrati in rete della pubblica amministrazione e per lo scambio di esperienze e buone pratiche
- rispettino le regole e le procedure generali concordate con la Regione per lo sviluppo ed il funzionamento della RUPAR
- si attrezzino al loro interno per assicurare il pieno e corretto utilizzo della Rete e dei servizi applicativi.

Il Centro Tecnico imposta il proprio modello produttivo ed organizzativo facendo riferimento, con gli accomodamenti del caso, al Centro Tecnico della Rete Nazionale. Le sue attività sono dettate:

- dalle disposizioni della Regione;
- dalle esigenze, dalle priorità e dalle disponibilità economiche delle Amministrazioni, Regione compresa;
- dalle scelte architetturali e progettuali prese a livello di Rete Nazionale e dagli Organismi nazionali di coordinamento;
- dalle norme in materia di servizi di telecomunicazione.

Ai fornitori è richiesto, oltre che la massima diligenza e professionalità nella realizzazione delle forniture di beni e servizi, un'ampia disponibilità a collaborare con la Regione, il Centro Tecnico e le Amministrazioni non solo sul piano della realizzazione e della gestione della Rete ma anche su quello della sua evoluzione tecnologica e dello sviluppo dei servizi applicativi.

B Specificazione tecnica ed operativa dei servizi di base

B.1 Il servizio di trasporto

B.1.1.1 Descrizione generale

Il servizio di trasporto deve garantire alle Amministrazioni la possibilità di collegare il proprio dominio a quello della RUPAR secondo le specifiche previste dal presente documento.

Il servizio di trasporto è fornito da un FSR abilitato che ha la responsabilità di garantire l'interconnessione a livello **EPO-LP** con gli altri FSR abilitati.
Tale interconnessione è prevista unicamente in tecnologia TCP/IP come successivamente specificato e quindi si intende per FSR il fornitore che gestisce l'interconnessione dell'Ente a livello TCP/IP, indipendentemente dai supporti trasmissivi di livello inferiore al protocollo IP che esso utilizza e che può acquistare/noleggiare da un qualsiasi fornitore di servizi di telecomunicazione regolarmente operante in Italia in base a licenza concessa dal Ministero delle Poste e Telecomunicazioni.

Gli FSR abilitati sono tenuti a comunicare al Centro Tecnico le eventuali evoluzioni delle loro offerte di servizi di trasporto per l'interconnessione a RUPAR, affinché esse siano vagliate come ammissibilità tecnica e come compatibilità di costi per essere poi inserite nel repertorio delle offerte usufruibili da parte delle Amministrazioni.

Gli FSR abilitati sono invitati a comunicare al Centro Tecnico anche le loro offerte di servizi per la realizzazione delle reti di dominio, affinché il CT possa esplicare la propria azione di consulenza e di informazione nei confronti delle Amministrazioni.

Ogni Amministrazione deve collegarsi a RUPAR mediante i servizi di un unico FSR e non può dotarsi di ulteriori collegamenti a Internet.

B.1.1.2 Definizione tecnica

Il Servizio di Trasporto della RUPAR si basa su cinque punti di interconnessione definiti **EPO-LP** (Exchange Point Operator – Locale Privato), uno per ogni capoluogo di provincia, gestiti direttamente dal Centro Tecnico.

Un EPO-LP della RUPAR è costituito da un armadio per apparati di comunicazione contenente uno switch Gigabit/Fast-Ethernet ad alte prestazioni.

Allo switch si interconnettono i router degli FSR che operano in quella provincia: i router saranno ospitati all'interno dell'armadio.

Ogni FSR ha diritto di allocare nell'armadio dell'EPO-LP un solo router dotato di una scheda Fast-Ethernet/Gigabit-Ethernet, che lo collega allo switch, e di una scheda per connessione a linea geografica, che collega lo collega al resto della rete del FSR e, per suo tramite, agli Enti suoi clienti.

L'accesso all'armadio dell'EPO-LP e la gestione dello switch sono di competenza del CT che supervisionerà anche il funzionamento dell'intero EPO-LP controllando l'interscambio di informazioni tra i router, che saranno gestiti ognuno dal proprio FSR.

La scelta del collegamento all'EPO in Gigabit Ethernet o in Fast Ethernet è lasciata al FSR che la farà in dipendenza del volume complessivo del traffico scambiato nell'EPO e del rispetto dei requisiti sulla Banda Minima Garantita enunciati nel seguito del presente documento.

La seguente figura mostra la struttura di un EPO-LP.

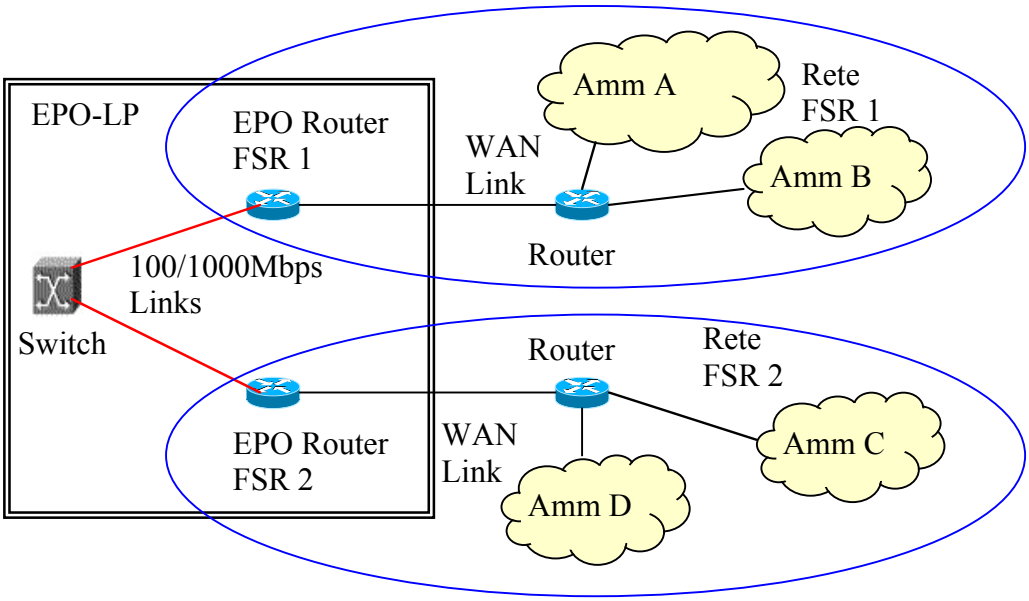


Figura 5. Schema di un EPO-LP della RUPAR

La figura successiva illustra la topologia della rete, le modalità di interconnessione degli FSR (ne sono mostrati tre per semplicità) e le modalità di interconnessione delle Amministrazioni alle reti degli FSR che costituiscono la RUPAR.

Nella figura la aree contornate da linea tratteggiata corrispondono alla rete propria di un FSR che eroga servizio di trasporto ad alcune Amministrazioni e si connette in corrispondenza degli EPO alle reti degli altri FSR: la figura è solo esemplificativa.

In questo esempio la connessione dei servizi tra la Amm-E e la Amm-D avverrà per mezzo dell'EPO di Brindisi, tra la Amm-H e la Amm-I per mezzo dell'EPO di Foggia e tra le Amministrazioni C e A avverrà per tramite l'EPO di Bari cui afferiranno le due reti dei FSR interessati, mentre la connessione tra le Amministrazioni servite da un medesimo FSR si potrà svolgere interamente all'interno della rete del FSR a cui hanno scelto di collegarsi.

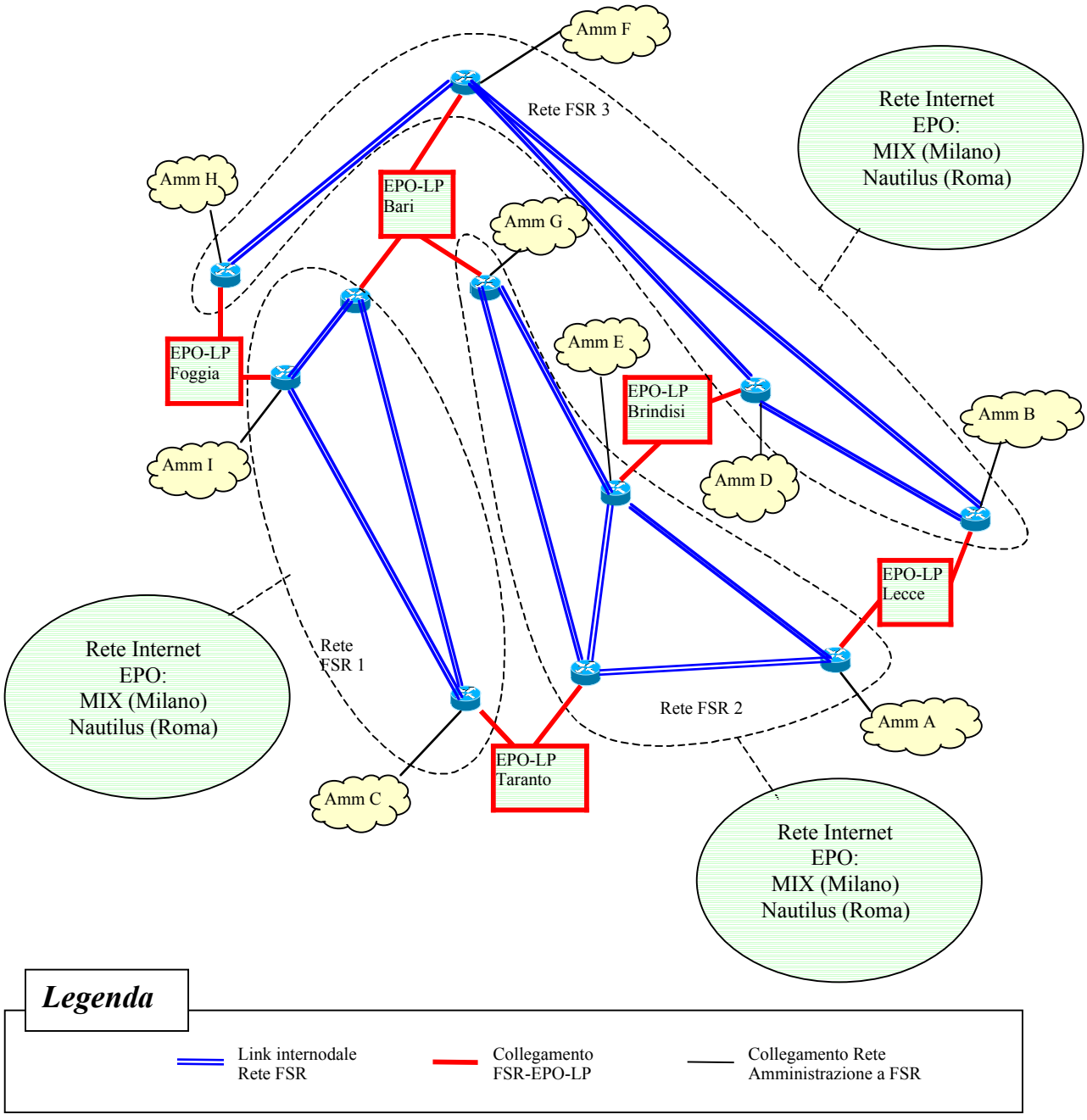


Figura 6. Schema complessivo della RUPAR

Le regole cui gli FSR si devono uniformare sono le seguenti:

- esistono cinque EPO Locali Privati, uno per ogni provincia, ognuno dei quali supporta il traffico di interscambio tra gli FSR per gli Enti localizzati in quella provincia;
- l'EPO di Bari ha funzioni anche di interscambio interprovinciale, nonché di interconnessione ad altre comunità nazionali e di backup degli altri EPO in caso di loro guasto;
- ogni FSR deve essere interconnesso all'EPO di Bari e ad almeno un altro EPO provinciale;
- il servizio di trasporto a livello provinciale deve essere garantito "Full-bandwith", quindi senza limitazioni di banda per gli Enti che interoperano a livello provinciale (ovviamente l'unico limite è quello della velocità di accesso scelta dal singolo Ente verso il FSR);
- per ogni Ente il FSR deve specificare nell'offerta e garantire nel servizio i due essenziali parametri di Banda Minima Garantita (BMG) verso l'EPO di Bari e verso l'Internet nazionale (servizio questo offerto direttamente dal FSR), intesa come accesso al **MIX** (**MI**lan e**X**change) di Milano ed eventualmente anche al **Nautilus** di ROMA. Oltre a questi due parametri principali, il FSR indicherà nell'offerta e garantirà nel servizio la BMG verso l'Internet internazionale (principali backbone europei e americani);

- per la corretta operatività degli EPO, i FSR dovranno disporre di un adeguato numero di reti ufficiali di classe C riservate al solo servizio RUPAR, per la gestione degli indirizzi degli Enti clienti, ed infine utilizzare il protocollo **BGP-4** per il routing negli EPO;
- il routing BGP-4 che verrà effettuato negli EPO concernerà esclusivamente le reti private (assegnate dal CT per la parte Extranet della RUPAR) e pubbliche (reti di classe C di proprietà degli FSR e riservate alla RUPAR) che verranno definite come appartenenti ad **Autonomous System privati** (AS numeri da 64512 a 65535, cfr. RFC1930);
- gli stessi FSR dovranno poi annunciare le reti pubbliche di classe C di propria pertinenza per il servizio RUPAR sull'Internet nazionale ed internazionale mediante la propria connessione ad Internet ed i propri Autonomous System ufficiali;
- deve esistere un **disaccoppiamento** tra il routing BGP-4 privato della RUPAR ed il routing a livello di Internet: questo risultato può essere ottenuto da un FSR semplicemente annunciando in modo statico nella propria rete globale connessa a Internet, la parte ufficiale della rete RUPAR di propria pertinenza.

Oltre a queste regole che concernono il funzionamento stesso della rete e dei protocolli di instradamento, si prevede che gli FSR debbano uniformarsi alle seguenti regole di gestione:

1. In generale tutti i router degli FSR devono consentire l'accesso in sola lettura via protocollo SNMP da parte del sistema centrale di controllo del CT, il cui indirizzo verrà comunicato allo FSR al momento dell'abilitazione ad operare: il sistema centrale di controllo del CT farà uso, oltre che del protocollo SNMP, anche del protocollo ICMP;
2. Ogni FSR dovrà fornire al CT i MIB estesi dei propri apparati al fine di consentirne il completo monitoraggio da parte del CT e dovrà inoltre consentire, qualora reputato necessario dal CT, l'installazione di *probe* (sonde di traffico) sulle interfacce dei propri router connessi alla RUPAR;
3. Ogni FSR deve attivare un proprio Centro di Gestione (CG-SR) attivo 365 giorni l'anno h24, con un numero telefonico a disposizione dei propri utenti ed un'altro a disposizione del CT e degli altri Centri di Gestione. Il CG-SR è tenuto a collaborare con il CT e con gli altri Centri di Gestione al fine di eliminare qualsiasi malfunzionamento della rete e di consentire l'ottimizzazione del traffico.

B.1.2 Funzionalità previste

E' stato già definito che l'interconnessione degli FSR è basata esclusivamente sul protocollo IP, ma ovviamente essi realizzeranno il servizio mediante circuiti portanti di tecnologia diversa.
In generale gli FSR potranno offrire tutti i servizi di telecomunicazione basati su circuiti portanti di cui sia ammessa dalla legislazione vigente la vendita al pubblico.

A solo titolo esemplificativo si indicano qui le tecnologie trasmissive considerate attuali:

- circuiti dedicati CDN e xDSL
- accessi permanenti in tecnologia Frame Relay e ATM
- accessi commutati analogici V.90
- accessi commutati numerici ISDN

Ad esse si aggiungeranno le tecnologie *Wireless Local Loop* non appena ammesse dal competente Ministero.

B.1.3 Modalità tecniche di erogazione

Sul collegamento della rete di dominio dell'Amministrazione con la rete del FSR fornitore, dovranno essere garantiti i livelli di servizio di trasporto e specificatamente la Banda Minima Garantita (BMG) verso i quattro seguenti principali snodi di trasporto, che tipicamente sono raggiungibili attraverso altrettanti circuiti virtuali:

- all'EPO provinciale (*BMG-Prov* = 1° frazione della velocità della linea di collegamento al FSR)
- all'EPO regionale (*BMG-Reg* = 2° frazione della velocità della linea di collegamento al FSR)
- a Internet nazionale (*BMG-Naz* = 3° frazione della velocità della linea di collegamento al FSR)
- a Internet internazionale (*BMG-Int* = 4° frazione della velocità della linea di collegamento al FSR)

Le somma delle quattro BMG può essere superiore ad 1, intendendo ovviamente che quei valori non siano ottenuti simultaneamente, in ogni caso deve essere garantito che, in assenza di traffico sulle altre direttrici, il traffico verso l'EPO provinciale possa effettuarsi senza limitazioni di banda (Full Bandwith), intendendo con questa dizione una garanzia di banda molto elevata che però potrebbe non essere esattamente pari a 100% per una serie di limitazioni tecniche.

Può accadere in certe configurazioni che il numero dei circuiti virtuali sia inferiore a quattro qualora uno di essi assolva più funzioni (p. es. la BMG-Naz e la BMG-Int siano coincidenti).

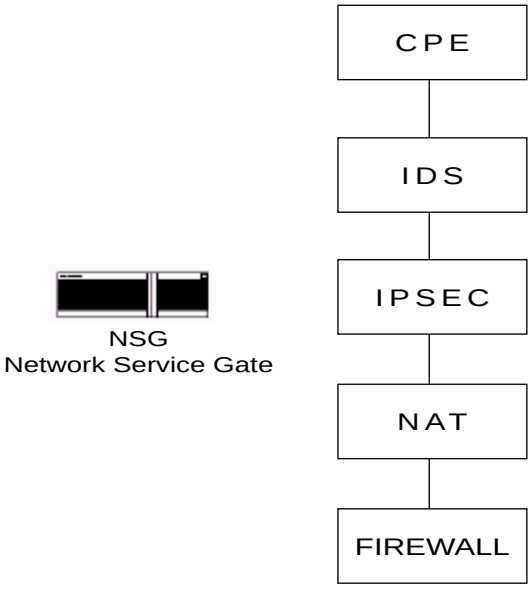
La modalità tecniche di erogazione del Servizio di Trasporto concernono inoltre le modalità di instradamento del traffico (routing).

Le principali regole concernenti il routing sono le seguenti:

- ogni FSR deve realizzare negli EPO cui è collegato sessioni di peering BGP-4 privato con tutti gli altri fornitori; su queste sessioni deve essere scambiato traffico concernente esclusivamente le reti RUPAR;
- le reti RUPAR apprese da un FSR negli EPO non devono essere propagate nella propria infrastruttura al di là della parte che contiene le utenze RUPAR; il traffico di utenti non RUPAR collegati ad un FSR verso Enti RUPAR collegati mediante altro FSR deve seguire il normale flusso sul backbone Internet nazionale per transitare sulla rete dell'altro FSR;
- le reti di classe C di un FSR, corrispondenti agli Enti gestiti da quello FSR in una specifica provincia, annunciate via BGP-4 negli EPO della Provincia e in quello di Bari sono apprese dagli altri FSR nell'EPO della Provincia e in quello di Bari. Poiché l'EPO di Bari ha la funzione di backup degli EPO provinciali, è opportuno che

gli FSR gestiscano in modo dinamico instradamenti multipli e variabili nel tempo (adozione di un IGP).

La seguente figura schematizza la configurazione funzionale della **PdR** (**Porta di Rete**), che è conforme a quella prevista per la RN:



Dove le diverse funzionalità possibili sono mostrate in modo completo:

- CPE, Customer Premises Equipment: router di collegamento
- IDS, Intrusion Detection System: componente di sicurezza per la rilevazione delle intrusioni
- IPSEC, funzione di realizzazione delle reti private virtuali (VPN)
- NAT, Network Address Translator: convertitore degli indirizzi di rete (tipicamente da privati a pubblici)
- Firewall: componente di sicurezza perimetrale per il controllo degli accessi alla rete

La successiva figura invece mostra un layout della PdR nel caso di uno schema molto completo in termini di reti di erogazione di servizi:

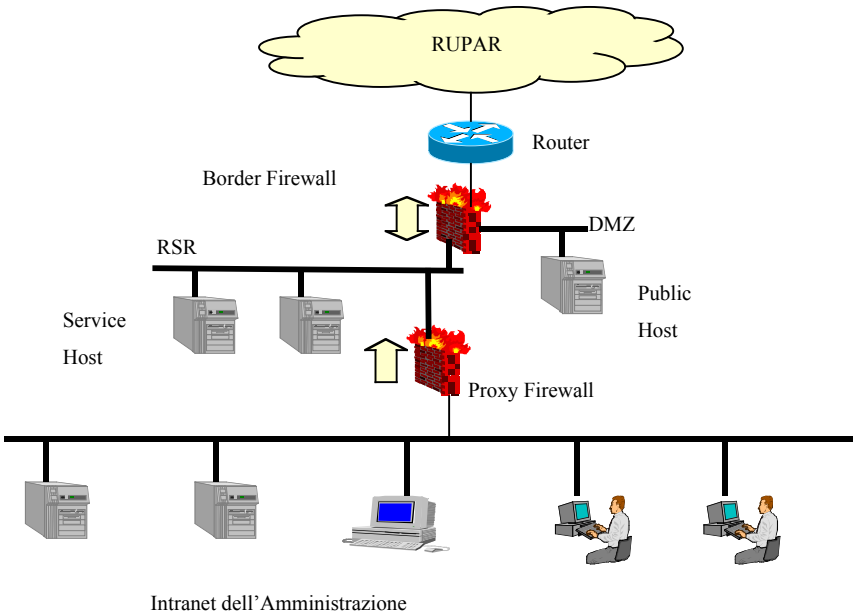
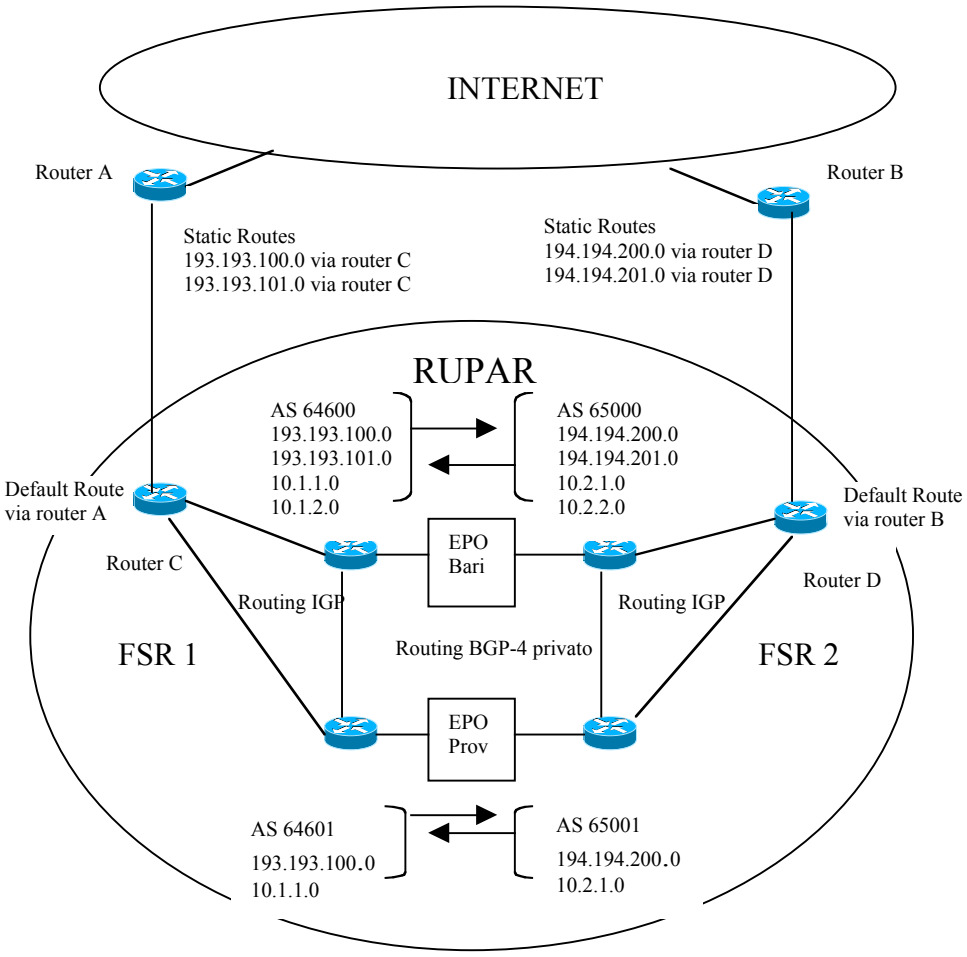


Figura 8. PdR con reti di servizio

La successiva figura mostra in modo schematico una possibile interazione a livello di routing tra due FSR sulla RUPAR e verso Internet.



Reti ufficiali gestite da FSR 1
193.193.100.0
193.193.101.0

Reti private RUPAR gestite da FSR 1
10.1.1.0
10.1.2.0

AS privati RUPAR gestiti da FSR 1
AS 64600
AS 64601

Reti ufficiali gestite da FSR 2
194.194.200.0
194.194.201.0

Reti private RUPAR gestite da FSR 2
10.2.1.0
10.2.2.0

AS privati RUPAR gestiti da FSR 2
AS 65000
AS 65001

Figura 9. Esempio di routing su RUPAR

Secondo questa impostazione il protocollo di routing BGP-4 risponde pienamente alle esigenze di gestire il routing negli EPO tra i diversi FSR, garantendone l'indipendenza tecnica ed operativa (p. es. scelta di diversi IGP), e contemporaneamente consentendo di gestire in modo razionale l'instradamento nella RUPAR sia delle reti private assegnate dal CT sia delle reti ufficiali che ogni FSR ha in propria dotazione.

L'esempio in figura mostra che tutte le reti di un FSR sono annunciate sull'EPO di Bari, mentre gli annunci su ogni EPO provinciale concernono le sole reti di quella provincia, realizzando così sia l'efficienza di instradamento del traffico che si svolge interamente a livello locale quando applicabile, sia la funzione di ridondanza degli EPO provinciali svolta dall'EPO di Bari.

L'utilizzo di Autonomus System privati nella RUPAR è opportuno dato il carattere riservato dell'infrastruttura (Extranet della PAL pugliese): nell'esempio in figura questa scelta ha soprattutto motivazioni di ordine formale, dato che è realizzato una separazione del routing verso Internet mediante l'adozione di rotte statiche tra i router che collegano la RUPAR ad Internet per conto di ognuno degli FSR (router A e C per FSR-1 e router B e D per FSR-2).
Si sottolinea che i router che svolgono servizio per la RUPAR, su cui è attivo il protocollo IGP che ne gestisce le reti, devono essere **riservati** alla RUPAR e non possono essere condivisi con altre reti

Rispetto alla configurazione tipica di una PdR mostrata in Figura 8. una buona politica minima di sicurezza prevede che il Firewall sia istruito a consentire l'accesso alla rete RSR solo ad indirizzi mittenti appartenenti alle reti private della RUPAR (reti tipo 10.0.0.0 nell'esempio di Figura 9). Questo tipo di regola ha il vantaggio di essere stabile, indipendente dai dettagli variabili delle configurazioni che possono essere effettuate dai diversi FSR, e coerente con l'idea della RUPAR come Extranet della PAL pugliese.

Va però precisato che in questa ipotesi il Proxy che permette l'accesso alla RUPAR alle stazioni dell'Intranet di una Amministrazione (nella citata Figura 8.il Proxy ed il Firewall coincidono) deve assumere all'esterno un indirizzo privato della RUPAR, in modo da avere libero accesso alle varie RSR.

Ne consegue allora che per poter far accedere ad Internet le stesse stazioni, il FSR interessato dovrà provvedere ad attivare, in corrispondenza dell'uscita dalla RUPAR e quindi nei router C e D per i due FSR della Figura 9., una funzionalità di NAT (Network Address Translation) per i proxy delle Amministrazioni da lui servite.

In base a questo approccio si può notare come le stazioni personali (client) di un'Amministrazione si presentino su Internet con un doppio livello di mascheramento, il primo effettuato dal proxy che maschera l'indirizzo Intranet della stazione trasportando tutte le sessioni sul proprio indirizzo privato RUPAR, e il

secondo effettuato dal router di frontiera RUPAR del FSR che maschera ogni indirizzo di server proxy mappandolo su un indirizzo ufficiale da lui gestito.

Viceversa si ritiene opportuno che gli elaboratori della DMZ di ogni Amministrazione siano dotati direttamente di indirizzo ufficiale (come mostrato in Figura 8.), in modo che la risoluzione dei loro nomi sia univoca in tutti gli ambiti (RUPAR e Internet).

L'infrastruttura descritta sarà quindi caratterizzata dalle seguenti funzionalità:

- le reti RUPAR dei servizi esterni (DMZ) saranno annunciate su Internet ognuna dal FSR che le controlla
- ognuna delle reti ***private*** RUPAR sarà normalmente raggiungibile da un'Amministrazione da due percorsi, ognuno con peso e/o "profondità" differente: in condizioni normali prevale l'annuncio proveniente dall'EPO Provinciale se presente (il che significa che la rete serve altra Amministrazione della stessa provincia e l'EPO provinciale è attivo), altrimenti dall'EPO-BA
- ognuna delle reti ***ufficiali*** RUPAR sarà normalmente raggiungibile da un'Amministrazione da tre percorsi, ognuno con peso e/o "profondità" differente: in condizioni normali prevale l'annuncio proveniente dall'EPO-Provinciale se presente (il che significa che la rete serve altra Amministrazione della stessa provincia ed il EPO provinciale è attivo), altrimenti dall'EPO-BA; in ogni

caso, pur non dovendosi mai porre l'esigenza per quanto descritto nel seguito, sarà sempre raggiungibile via default route sull'Internet nazionale

- l'EPO-BA rappresenta il back-up dell'EPO-Provinciale, nonché l'accesso ad altre comunità di PA esterne ed ai servizi centrali di supporto alla cooperazione applicativa: si prevede che la sua architettura sia tale da escludere un suo totale blocco

Per quanto concerne il collegamento ad altre comunità di PA esterne alla RUPAR Puglia e di comune utilità, esso verrà gestito dal CT-RUPAR in accordo con il CT della RN.

Qualora un Ente dovesse rescindere il contratto che lo lega a un FSR per attivarne uno con un altro FSR, dovrà necessariamente modificare gli indirizzi numerici dei propri elaboratori di servizio, se allocati presso il suo collegamento al servizio di trasporto.

L'EPO-BA sarà realizzato con un'architettura **completamente ridondante** in modo da garantire la continuità di servizio in ogni circostanza.

A questo fine l'EPO-BA sarà allocato presso il CT e sarà strutturato in due armadi tecnologici allocati in due diversi edifici del Parco Scientifico Tecnopolis (Valenzano, Bari) che ospiterà l'infrastruttura tecnologica del CT.

Questa collocazione consentirà di sfruttare le potenti *facilities* dell'infrastruttura del Parco:

- collegamenti in fibra ottica tra edifici remoti
- rete di alimentazione elettrica con gruppi di UPS e generatori di emergenza differenziati per gruppi di edifici
- collegamenti a reti telematiche di fornitori di servizi di telecomunicazione disponibili su percorsi fisici differenziati su cavi in rame, cavi in fibra ottica e ponte radio
- sistemi antincendio, di sorveglianza e di allarme presidiati h24 da personale di guardia

conferendo all'EPO di Bari quella configurazione completamente ridondata ad **alta disponibilità** che è indispensabile per garantire la funzionalità della RUPAR con la continuità di servizio necessaria.
Va inoltre considerato che questa configurazione consente di ottenere anche la massima sinergia con l'infrastruttura tecnologica del Centro Tecnico preposta a fornire i servizi di supporto alla cooperazione applicativa.

Questa infrastruttura tecnologica sarà anch'essa strutturata come un Centro Servizi ad Alta Disponibilità, dotato di tutte le necessarie ridondanze in un contesto di dislocazione fisica, che garantisca l'operatività dei servizi anche in caso di eventi disastrosi.

B.1.4 Standard tecnici di riferimento

Il servizio di trasporto, così come definito nel presente documento, si attua a livello RUPAR, e quindi negli EPO Locali Privati, esclusivamente mediante il protocollo IP.
Tra gli standard tecnici di riferimento saranno quindi certamente presenti quelli relativi ai protocolli TCP/IP, tuttavia poiché è richiesto che gli FSR rendano disponibili circuiti di accesso alla RUPAR basati sui servizi di comunicazioni la cui vendita al pubblico è ammessa dalla normativa vigente, ne consegue che anche gli standard tecnici che regolamentano tali servizi di comunicazione sono vincolanti per gli FSR.

Peraltro i servizi di comunicazione sono regolamentati sia da standard "de jure" emessi da Enti pubblici nazionali e internazionali, sia da standard "de facto" governati da Enti privati ("Forum") costituiti da accordi industriali dei fornitori delle specifiche tecnologie; è scopo del presente capitolo indicare, più che un elenco esaustivo dei singoli standard applicabili, gli Enti che sono considerati di riferimento per le specifiche tecnologie.

B.1.4.1 Standard TCP/IP

Gli standard tecnici di riferimento relativi ai protocolli TCP/IP sono quelli emanati dal competente Centro di gestione tecnica della rete Internet: IETF (Internet Engineering Task Force: URL: **http://www.ietf.org**).

In generale e' richiesto agli FSR di adottare gli standard tecnici una volta emanati dall'IETF, solo in qualche caso eccezionale potrà essere avviata dal CT una procedura per arrivare all'adozione anticipata, con il consenso di tutti i Fornitori interessati, di uno standard ancora in via di approvazione definitiva da parte dello IETF.
Lo standard IETF è in genere specificato mediante la sigla RFC (Request For Comment) del documento che lo specifica, il quale va considerato unitamente agli eventuali documenti successivi che lo rendono obsoleto, modificandolo e integrandolo.

La versione del protocollo IP adottata dalla RUPAR è la versione 4, attualmente utilizzata dalla totalità della rete Internet, per una eventuale adozione della versione 6 si rimanda al capitolo sulle "**Prospettive evolutive**" della RUPAR.

Poiché l'interazione tra diversi fornitori a livello RUPAR si realizza negli EPO, è di fondamentale importanza il supporto del protocollo BGP-4 (RFC1771, "A Border Gateway Protocol") e della gestione dell'aggregazione degli indirizzi CIDR (RFC1519, "Classless InterDomain Routing").

B.1.4.2 Standard dei servizi di comunicazioni

Per ognuno dei servizi di comunicazioni supportati sono rilevanti, oltre agli standard prescritti dal regolamento tecnico del servizio come approvato dal competente Ministero, gli standard dell'IETF che specificano le modalità del trasporto del TCP/IP sul servizio in questione: p. es. PPP (RFC1661, "Point to Point Protocol") per il trasporto su linee seriali e MPPP (RFC1717, "Multilink PPP") per l'aggregazione di più link in parallelo per realizzare un unico collegamento a velocità più elevata.

In generale per le tecnologie di trasmissione a livello locale e geografico sono rilevanti gli standard emessi da:

- IEEE (Institute of Electrical and Electronics Engineers, URL: http://www.ieee.org) normalmente recepiti dall'ISO (International Standard Organization, URL: http://www.iso.ch)

- ETSI (European Telecommunication Standard Institute, URL: http://www.etsi.org)
- ITU-T (International Telecommunication Union-Telecom, URL: http://www.itu.int/ITU-T/)
- ATMForum (URL: http://www.atmforum.com)
- FrameRelayForum (URL: http://www.frforum.com)

B.1.5 Qualità di servizio

La qualità tecnica del servizio nel caso del Servizio di trasporto si misura mediante le seguenti metriche:

1. disponibilità del servizio
2. prestazioni dei collegamenti

La disponibilità del servizio è misurata in base ai due parametri di ***Uptime*** (Tempo ininterrotto di disponibilità di un servizio) e **MTBF** (Mean Time Between Failures, tempo che intercorre tra due guasti consecutivi dello stesso servizio).
La disponibilità di base richiesta è di 24 ore al giorno e 365 giorni l'anno.

I valori previsti sono i seguenti:

1. Uptime > 99,5%
2. MTBF > 2000 ore

Si noti che il parametro di Uptime è comprensivo anche degli interventi, con caratteristiche bloccanti del servizio, programmati per finalità di manutenzione preventiva e/o evolutiva.

Per le prestazioni dei collegamenti i due parametri fondamentali sono il rispetto della BMG (Banda Minima Garantita) e il tasso di perdita di pacchetti.
Utilizzando come unità campione una sequenza (> 10) di pacchetti Ping (ICMP Echo) sincroni di dimensione 8000 bytes, la verifica dei parametri consiste nella rilevazione, per tutti i circuiti virtuali su cui sia garantita una BMG, delle seguenti grandezze:

1. **RoundTripDelay** < C*128/BMG sec (dove C=1,2 per il collegamento all'EPO-LP provinciale e C=1,5 per gli altri; il RoundTripDelay è il tempo di risposta medio fornito dallo strumento/comando "**ping**" espresso in secondi; la BMG è espressa in Kbit/sec)
2. **Tasso di perdita** < 0,1%

3. **Tempo di download/upload** < C*8*DimensioneFile/BMG sec. (C=1,2 DimensioneFile è espressa il Kbytes e la BMG in Kbit/sec).

Per i collegamenti di tipo commutato si richiede inoltre che la probabilità di trovare la linea occupata debba essere inferiore al 1% in entrambe le fasce orarie 08:00-20:00 e 20:00-08:00

B.2 Il servizio di interoperabilità di base

Il Servizio di Interoperabilità di base è fornito anch'esso dai FSR abilitati dal CT. Ogni Amministrazione deve essere servita da un unico FSR che erogherà nei suoi confronti sia il Servizio di Trasporto che il Servizio di Interoperabilità da Base.

Il FSR può erogare i propri servizi di interoperabilità in tre diverse configurazioni:

- in modo totalmente centralizzato mediante uno o più propri Centri Servizi connessi a RUPAR a cui le Amministrazioni clienti si collegano in modo trasparente
- in modo distribuito mediante l'allocazione di risorse elaborative presso la connessione in RUPAR delle Amministrazioni
- in modo misto, con alcuni servizi allocati presso le Amministrazioni ed altri centralizzati

In tutti i casi il FSR è responsabile della erogazione della totalità dei servizi di interoperabilità di base previsti, nonchè del supporto (housing e sicurezza) dei servizi applicativi che dovessero essere attivati dall'Amministrazione sull'infrastruttura dei servizi di interoperabilità di base.

Il FSR che serve un'Amministrazione è sempre il responsabile dell'attuazione delle politiche di sicurezza per quella Amministrazione.

La seguente figura illustra lo schema di riferimento della Porta di Rete (PdR).

Questo schema è valido in tutte le tre configurazioni precedentemente indicate, con l'avvertenza che nel caso di servizi allocati nel Centro Servizi gli elaboratori che forniscono i servizi di Interoperabilità di base possono essere condivisi tra più Amministrazioni.

Va precisato che in quest'ultimo caso in cui i servizi siano allocati presso il Centro Servizi dello FSR, l'intera infrastruttura di elaboratori di servizio deve essere riservata ai servizi RUPAR.

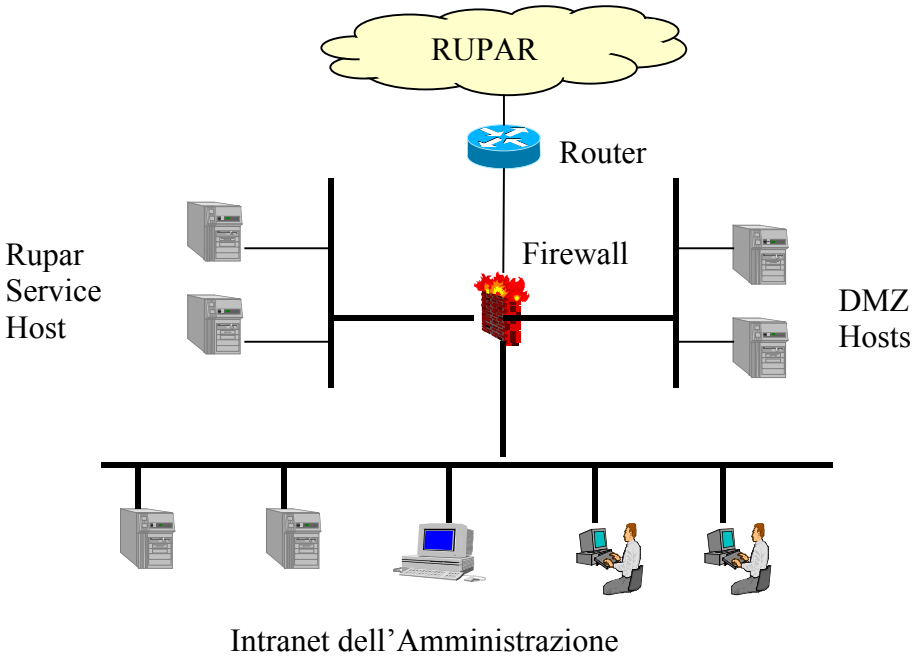


Figura 10. Schema della PdR

Gli oggetti mostrati in figura hanno principalmente valenza funzionale e possono essere compresi in un numero minore di apparati in dipendenza della effettiva realizzazione fisica del punto di accesso.

Il router è la funzione che gestisce l'interconnessione a livello di trasporto.

Il Firewall ha il compito di garantire la sicurezza del dominio dell'Amministrazione, filtrando le richieste di connessione provenienti dall'esterno per minimizzare la possibilità che queste

richieste siano di tipo pericoloso per l'Amministrazione; esso consente tipicamente un traffico bidirezionale controllato in quanto deve consentire sia all'utenza dell'Amministrazione di "uscire" sulla RUPAR per accedere ad altre Amministrazioni e/o ad Internet, sia all'utenza esterna di "entrare" per accedere ai servizi offerti da questa Amministrazione per mezzo dei suoi "Service Hosts".

Alle spalle del Firewall si trovano tre reti:

- la zona demilitarizzata (DMZ, **D**e**M**ilitarized **Z**one), che è così definita in quanto la sua difesa non può essere totale dovendo essa ospitare gli elaboratori (Service Hosts) preposti all'erogazione di servizi di applicativi offerti dall'Amministrazione agli utenti esterni (utenti Internet) ed ovviamente accessibili anche alle altre Amministrazioni. Sulla rete DMZ i Service Host hanno indirizzi ufficiali Internet.
- la **R**ete dei **S**ervizi **R**UPAR (RSR) che è riservata ai servizi di interoperabilità e cooperazione applicativa tra Amministrazioni e quindi **non** è accessibile da Internet ma solo dalle altre reti RUPAR
- la rete interna (Intranet) che ospita il dominio dell'Amministrazione, da cui il Firewall consente esclusivamente un traffico in uscita dal dominio dell'Amministrazione, per permettere all'utenza dell'Amministrazione di "uscire" sulla RUPAR per accedere ad altre Amministrazioni e/o ad Internet. Questa funzionalità, denominata

Proxy è specificatamente responsabile anche di "nascondere" gli indirizzi degli elaboratori interni, rendendo noto all'esterno esclusivamente il proprio indirizzo. La sua tipica funzionalità di protezione è semplicemente quella di blocco totale di tutte le connessioni entranti. Dal punto di vista dell'indirizzamento la rete interna della PAL è amministrata con indirizzi di rete privata (p. es. network 10.0.0.0) dato che i suoi host **non** sono accessibili né da Internet né dalla Extranet della RUPAR; il Firewall protegge questa rete e svolge funzioni di proxy (e eventualmente di NAT, **N**etwork **A**ddress **T**ranslation) per consentire alle stazioni client di accedere a servizi esterni.

Una generica PdR può non prevedere la possibilità di offrire servizi all'esterno ed in tal caso non prevederà una DMZ, così come può prevedere di offrire verso l'esterno un'unica tipologia di servizi utili sia all'utenza esterna (cittadini) che alle altre Amministrazioni e in tal caso non sarà necessaria la presenza di una RSR. In ogni caso presso la PdR sarà sempre presente almeno la funzione basilare di Firewall/Proxy che interconnette a RUPAR e a Internet il dominio di un'Amministrazione.

A questo fine e per evitare possibili confusioni si definisce con precisione il **PdR** dell'Amministrazione come il punto in cui è allocata questa funzione basilare di **Firewall/Proxy**.

La PdR, anche quando è configurata in modo completo comprensiva di DMZ e RSR, può anche non supportare, mediante i service hosts allocati nelle suddette reti, la totalità dei servizi di interoperabilità.
Si riconosce infatti che non tutti i servizi di interoperabilità sono caratterizzati dalle medesime esigenze di allocazione in prossimità della Intranet dell'Amministrazione.

Può accadere, per esempio, che l'accesso sicuro via WWW a servizi fondati su una banca dati gestita dall'Amministrazione, suggerisca l'allocazione del server WWW su una DMZ connessa in rete locale al DBMS server che ospita la banca dati e che è allocato nell'Intranet dell'Amministrazione: questo al fine di rendere più efficiente l'interazione sicura tra il WWW e il DBMS server.

Viceversa si può riconoscere che per esempio la funzione di DNS, deputata a risolvere i nomi dei service hosts allocati su DMZ e RSR, non ha in generale requisiti prestazionali tali da imporre la sua allocazione in prossimità dell'Intranet dell'Amministrazione e quindi è un possibile candidato all'allocazione presso il Centro Servizi del FSR.

B.2.1 Funzionalità previste e modalità tecniche di erogazione

Le funzionalità sono state indicate nel capitolo A.2.2, suddivise in due gruppi.

B.2.1.1 Le funzionalità di interoperabilità tecnica

Gestione dei Nomi di Dominio (DNS)

Consiste nella gestione del dominio che identifica l'amministrazione nonchè di tutti i nomi degli elaboratori sulle reti di servizio (DMZ e RSR).

Successivamente alla fase di attribuzione, da parte del FSR, delle subnet di indirizzi IP necessarie al corretto funzionamento degli apparati e delle postazioni di lavoro della PAL, il FSR si adopererà per l'attivazione del dominio Internet dell'Amministrazione, oltre che della predisposizione del Proxy/Firewall e degli altri servizi di interoperabilità.

Come già evidenziato in precedenza, a differenza del collegamento Internet (che viene sempre incluso nell'offerta di servizio di trasporto), la singola PAL potrebbe non richiedere immediatamente la predisposizione di una rete DMZ e/o di una rete RSR. Pertanto, nella successiva lista delle funzionalità si dovrà tener conto di questa evenienza.

Recepito dalla PAL il nome del dominio da attivare, il FSR dovrà:

- garantire la fruizione del servizio di risoluzione dei nomi a tutte le postazioni del Dominio Amministrativo fornendo modalità tecniche di utilizzo;
- coordinare la gestione del *naming* per tutte le reti (DMZ, Intranet, RSR); in particolare, per un host raggiungibile da più reti (ad es. dalla rete Intranet della generica PAL e dalla rete Internet) dovrà essere utilizzato sempre lo stesso nome simbolico;
- su Internet, predisporre il DNS server primario per il nome del dominio individuato dalla PAL; quindi, predisporre almeno un DNS server secondario del precedente primario; nessun nome di host presente sulla Intranet e/o sulla rete RSR dovrà essere incluso nel database;
- sulla Intranet, soltanto se richiesto dalla PAL, predisporre il DNS server primario e secondario per il nome del dominio individuato dalla PAL, predisponendo meccanismi di *forward* per risolvere nomi esterni;
- sulla RSR, garantire la visibilità del DNS di riferimento gestito dal CT, che contiene le risorse RUPAR attivate sulla rete regionale;
- richiedere indirizzi e nomi di dominio validi prima di predisporre host sulla rete RSR.

Affinché le postazioni client della Intranet possano utilizzare i servizi di interoperabilità, il FSR dovrà fornire alla PAL indicazioni tecniche coerenti con la configurazione del Proxy/Firewall presente nella PdR.

Per risolvere i nomi degli host afferenti alle reti RSR il FSR dovrà predisporre all'occorrenza meccanismi di caching/forwarding per indirizzare il DNS delle risorse RSR gestito dal CT.

Nel caso in cui la PAL chiedesse la predisposizione di una LAN RSR, il FSR si farà carico della registrazione e dell'attivazione tecnica del subdomain RUPAR coordinandosi con il CT, in qualità di gestore del dominio di più alto livello.

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC1034, RFC1035, RFC2535 e successive estensioni.

Directory

Consiste nella gestione di classi di oggetti accessibili attraverso l'infrastruttura di servizi.
Come set minimo di informazioni, il servizio deve gestire l'anagrafica ed i recapiti telefonici e di email dei dipendenti dell'Amministrazione. Il servizio dovrà essere integrato da informazioni (attributi) pubbliche tipo "*public security keys*" non appena disponibili.

Il servizio, conforme alle specifiche X.500 e con il supporto del protocollo LDAP, verrà successivamente integrato con la posta elettronica fornendo così una rubrica di indirizzi degli utenti come parte integrante dell'infrastruttura di sicurezza (*Certification Authority*). Oltre al descritto LDAP server pubblico, al fornitore potrà essere richiesto di attrezzare e gestire un più completo LDAP server RUPAR sulla rete RSR. Mediante opzioni di replicazione parziale del server LDAP RUPAR si aggiornerà il server pubblico sulla rete DMZ.

La documentazione ufficiale (standard) di riferimento è la seguente: RFC1777, RFC2247 e loro aggiornamenti.

Tempo ufficiale di rete

Consiste nel gestire il recepimento del tempo ufficiale propagato dal CT sulla RUPAR e nella sua distribuzione a tutti gli elaboratori di servizio.

L'applicazione software che permetterà alle risorse di comunicazione ed elaborazione collegate alla RUPAR di sincronizzare i propri orologi è il **N**etwork **T**ime **P**rotocol **v**ersione **3**. Il protocollo sarà attivato in modalità sicurizzata per garantire sicurezza e autenticità del tempo.

La sincronizzazione dei clock sarà obbligatoria per tutti gli apparati di instradamento e per tutti gli "host services" mentre per le principali piattaforme client potranno essere impiegate soluzioni software conformi.
Il Time Server NTP primario della RUPAR verrà gestito dal CT presso l'EPO di Bari; i FSR sincronizzeranno i clock dei propri dispositivi presenti presso l'EPO e daranno origine ad una gerarchia di strati NTP indicati per sincronizzare gli orologi di tutti i dispositivi afferenti alla propria rete di trasporto.
La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC1305 e successivi aggiornamenti.

Gestione sistemi e rete

Consiste nella gestione sistemistica e nel monitoraggio di tutti i servizi erogati alle Amministrazioni.
Per l'attività di gestione sistemistica e monitoraggio dei server e degli apparati di networking, si dovrà prevedere l'utilizzo di soluzioni/metodologie client-server e più specificatamente "agent-manager" basate sullo standard IETF SNMP (Simple Network Management Protocol) ed RMON (Remote network MONitoring).

La gestione riguarderà specificatamente:

- i dispositivi presso la sede della generica PAL (concentratori di rete locale, router di comunicazione geografica, server Proxy, Firewall, host services);
- gli apparati che realizzano l'infrastruttura di trasporto;
- gli apparati dei Centri servizi (router, concentratori LAN, host services, Firewall).

I FSR dovranno autorizzare sessioni SNMP da/verso Manager SNMP gestiti dal CT.

Le attività di gestione saranno espletate secondo le prescrizioni del capitolo successivo e comunque rispettando gli standard IETF SNMP basate su community string (RFC1157).
Successivamente, potranno essere implementati modelli sicurizzati basati su SNMPv3 (RFC2570, non standard ed appartenente alla categoria "Informational").
Oltre ai citati, altri documenti ufficiali (standard IETF) sono: RFC1757 e RFC2021.

Sicurezza

La gestione della sicurezza che compete ai FSR concerne essenzialmente:

- i **Firewall** di protezione dei servizi;

- i sistemi **IDS** (Intrusion Detection System) addetti alla rivelazione di tentativi complessi di intrusione;
- i servizi di **VPN** (Virtual Private Network).

I Firewall sono preposti alla protezione dell'intero accesso all'esterno sia per i servizi che per le stazioni utente. E'essenziale che essi adottino tutte le opportune politiche di protezione come:

- sbarramento statico di tutte le porte applicative non destinate ad erogare servizio, al fine di limitare le possibilità di attacco agli elaboratori preposti all'erogazione dei servizi;
- sbarramento statico dell'accessibilità di specifiche reti a partire da altre reti: p. es. limitazione degli accessi ai servizi su reti RSR ai soli indirizzi privati della RUPAR;
- filtraggio in tempo reale del traffico con tecniche di ispezione a livello di protocollo (packet inspection) ed a livello di sessione (*stateful inspection*) al fine di garantire sia l'arresto di attacchi di tipo DOS (Denial Of Service) che il blocco di flussi informativi contenenti minacce di cui si riconosca la "firma";
- mascheramento delle stazioni client (legato al servizio di accesso a WWW o Proxy);
- abilitazione controllata di specifici flussi informativi non gestiti dal proxy;
- log delle sessioni per registrare lo sviluppo del traffico gestito.

I sistemi IDS rappresentano un secondo livello di protezione che si caratterizza come segue:

- la loro presenza è ignota ai potenziali aggressori e da loro non rivelabile, per cui sono potenzialmente ed intrinsecamente più sicuri del Firewall stesso;
- sono in grado di effettuare analisi sofisticate sul traffico, con metodologie tipiche di sistemi esperti, rivelando attacchi di struttura complessa;
- non rallentano l'attività di inoltro del traffico, dato che operano in modo passivo sulla rete (analisi del traffico in modo promiscuo o "*sniffing*") e non hanno il compito di smistare traffico;
- sono in grado di pilotare il Firewall stesso per attivare in tempo reale sbarramenti rispetto ad indirizzi mittenti individuati come fonte di aggressioni in corso;
- provvedono sia alla registrazione delle anomalie che alla generazione di allarmi verso il personale di gestione.

Le due tecnologie sono complementari ed il loro simultaneo impiego si giustifica in contesti dove sia presente una significativa offerta di servizi.

Le tecnologie VPN si rendono necessarie quando si ritenga che il traffico da gestire nei confronti di specifiche controparti debba essere integralmente protetto dalla possibile lettura di terze parti. Uno di questi casi può essere rappresentato per esempio dal desiderio di un'Amministrazione di usufruire di servizi informatici

interni (Contabilità, Personale etc.) in modalità ASP (Application Service Provider) su rete Internet.

In questo caso il collegamento con il fornitore di soluzioni ASP deve necessariamente essere configurato come un'estensione virtuale della rete Intranet dell'Amministrazione, il che può essere realizzato solo attivando una funzionalità di VPN sul Firewall, di concerto con il fornitore di servizi ASP.
Lo standard di riferimento per le **VPN** è l'**IPSEC** (RFC2401).

Poiché la tematica della sicurezza concerne non solo la gestione di specifici sistemi di protezione, come quelli menzionati, ma anche la corretta attuazione di politiche di sicurezza sui sistemi che erogano i servizi, è responsabilità del FSR di attuare le politiche prescritte su tutti i sistemi che ospitano i servizi da lui direttamente gestiti e descritti nel presente capitolo.
Per quanto concerne la sicurezza dei sistemi che ospitano i Servizi di Cooperazione Applicativa si rimanda allo specifico capitolo.

B.2.1.2 Le funzionalità di interoperabilità applicativa

Posta Elettronica

Consiste nella gestione di uno o più server di Posta Elettronica dove vengono definite le caselle postali del personale dell'Amministrazione accessibili sia da RUPAR che dall'esterno.
Il servizio osserverà alcuni principi generali:

- lo scambio di messaggi fra Amministrazioni RUPAR avverrà attraverso sessioni SMTP e/o ESMTP/(S)MIME prioritariamente utilizzando l'infrastruttura RUPAR;
- ogni utente avrà un solo indirizzo di email, sia per l'infrastruttura RUPAR che per Internet ed indipendentemente dallo standard di formato utilizzato;
- la posta smistata dal server di posta elettronica deve essere controllata per verificare l'eventuale presenza di virus (scanning), in caso affermativo la mail deve essere cancellata e deve essere inviata una notifica dell'accaduto a mittente e destinatari; il sistema antivirus deve essere dotato di aggiornamento automatico e frequente (almeno una volta alla settimana) delle liste di definizione dei virus.
- per supportare lo standard OSI X.400 devono essere attrezzati opportuni mail gateway tra lo standard X.400 e lo standard TCP/IP referenziato come standard RFC822;

- i server di posta possono essere ridondati e dovranno prevedere piena integrazione verso server LDAP (Directory server) e verso l'infrastruttura PKI non appena disponibili.

L'accesso al servizio sarà possibile da qualunque host RUPAR mediante:

- sessioni client/server tipo POP3/IMAP;
- sessioni HTTP;
- sessioni obbligatoriamente cifrate quando un dipendente di una Amministrazione vuole leggere la propria mailbox da un Dominio Amministrativo diverso da quello di appartenenza.

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC821, RFC1341, RFC1869, RFC1495, RFC2045, RFC1006, RFC2126, RFC2156 e loro aggiornamenti.

Accesso a WWW

Il servizio consente a tutti gli host della Intranet di ottenere informazioni ospitate su World Wide Web server remoti mediante il protocollo HTTP (HyperText Transfer Protocol). L'accesso è garantito attraverso un server proxy/cache HTTP localizzato nella PdR.

Il server proxy/cache dovrà gestire:

- proxying e caching di almeno HTTP, FTP e RTP;
- proxying per sessioni sicurizzate SSL;
- trasparent caching;
- autenticazione utente;
- "*access control list*" intese come liste/filtri per l'accesso al servizio;
- SNMP;
- caching di risoluzioni DNS.

Il servizio, amministrato dal FSR, osserverà alcuni principi generali:

- l'Amministrazione produrrà la lista degli utenti e/o delle postazioni di lavoro abilitate al servizio; questa regola verrà osservata anche per tutti gli altri protocolli/servizi;
- ad utente verrà attribuita una soglia di impiego della banda;
- il FSR configurerà e gestirà opportune "*black-list*" contenenti siti da contenuti potenzialmente dannosi, violenti e/o moralmente indicibili;
- il FSR dovrà fornire indicazioni su come configurare il servizio sui client del dominio dell'Amministrazione e dovrà garantire anche la configurazione automatica del browser di navigazione fornendo opportuna URL.
- i files scaricati aventi estensioni potenzialmente pericolose (p. es. .exe) devono essere controllati per verificare

l'eventuale presenza di virus (scanning), in caso affermativo il file non deve essere consegnato all'utente che deve essere informato da un messaggio visualizzato sul browser.

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC1945 e successivi aggiornamenti.

Trasferimento file

Il servizio consente a tutti gli host della RUPAR di scambiare file di dati, anche di grandi dimensioni, con sistemi remoti mediante il protocollo FTP (File Transfer Protocol). Dalla Intranet dell'Amministrazione l'accesso è garantito alle postazioni abilitate attraverso il server proxy descritto precedentemente mentre l'elenco delle postazioni da abilitare sarà fornito dall'Amministrazione.

Il servizio potrà essere utilizzato in modalità interattiva oppure essere integrato in altro servizio applicativo e sarà fruibile garantendo sempre le massime condizioni di sicurezza.

Salvo impedimenti oggettivi e/o ad eccezione di accessi a pubblici archivi, eventuali server FTP predisposti su reti RUPAR (DMZ o RSR) dovranno richiedere la cifratura della password durante l'autenticazione dell'utente (supporto AUTH command).

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC959 e suoi aggiornamenti.

Terminale virtuale

Il servizio consente a tutti gli host abilitati della RUPAR di effettuare sessioni di emulazione terminale con sistemi remoti mediante il protocollo TELNET e/o di Remote Shell. Dalla Intranet dell'Amministrazione l'accesso è garantito alle postazioni abilitate attraverso il server proxy descritto precedentemente mentre l'elenco delle postazioni da abilitare verrà fornito dall'Amministrazione.

Il servizio sarà fruibile garantendo sempre le massime condizioni di sicurezza.

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC854 e suoi aggiornamenti/estensioni.

Accesso a news

Il servizio consente a tutti gli host abilitati della RUPAR di partecipare al circuito di distribuzione dei bollettini di informazione (news) mediante il protocollo NNTP (Network News Transfer Protocol).

Dalla Intranet dell'Amministrazione l'accesso è garantito alle postazioni abilitate attraverso il server proxy descritto precedentemente mentre l'elenco delle postazioni da abilitare verrà fornito dall'Amministrazione.

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC977 e successivi aggiornamenti/estensioni.

B.2.2 Standard tecnici di riferimento

I servizi di interoperabilità, come definiti nel presente documento, vengono erogati su elaboratori afferenti le reti DMZ, RSR della RUPAR oppure, come nel caso del Proxy, presso la sede d'utente coincidente con la PdR.
Essi si basano sui servizi di trasporto e pertanto condivideranno con essi tutti gli standard di riferimento. Analogamente ai fornitori dei servizi di trasporto, i FSR adotteranno lo standard TCP/IP e recepiranno le raccomandazioni emanate da IETF.

B.2.3 Qualità di servizio

La qualità tecnica del singolo servizio di interoperabilità si misura mediante le seguenti metriche:

1. disponibilità temporale
2. prestazioni di erogazione

La disponibilità del servizio è misurata in base ai due parametri di ***Uptime*** (Tempo ininterrotto di disponibilità di un servizio) e **MTBF** (Mean Time Between Failures, tempo che intercorre tra due guasti consecutivi dello stesso servizio).

La disponibilità di base richiesta è di 24 ore al giorno e 365 giorni l'anno.

I valori previsti sono i seguenti:

1. Uptime > 99,5%
2. MTBF > 2000 ore

Si noti che il parametro di Uptime è comprensivo anche degli interventi con caratteristiche bloccanti del servizio, programmati per finalità di manutenzione preventiva e/o evolutiva.

Per tutti i servizi di interoperabilità si richiede che eventuali interruzioni per manutenzioni siano comunicate con un anticipo di almeno 3 giorni e siano programmate in giorni festivi.

Per le prestazioni di erogazione dei singoli servizi intendiamo la velocità con cui servizi interattivi o batch vengono fruiti dagli utenti in condizioni di rete normali.

Nel caso di servizi interattivi e relativamente alle prestazioni standard di trasferimento dati end-to-end del livello di trasporto in condizioni normali, le prestazioni dei servizi di interoperabilità potranno prevedere un ulteriore ***delay*** **non superiore al 5%** rispetto alle prestazioni ottenibili senza l'impiego del/i servizio/i di interoperabilità.

Per servizi batch, tipo le sessioni SMTP tra Mail Transfer Agent, le prestazioni complessive devono prevedere, oltre al delay definito in precedenza, anche una soglia di messaggi presenti nella outgoing spool directory dell'MTA; il numero di messaggi massimo nella coda di spool di un MTA non deve superare le dieci unità (sono esclusi i messaggi etichettati "*deferred*" a causa di indisponibilità del server SMTP di destinazione).

B.3 I servizi di supporto

Si tratta di tutti i servizi, complementari ai servizi di trasporto e interoperabilità, che sono resi disponibili sulla RUPAR sia dai Fornitori che dallo stesso Centro Tecnico.
Questi servizi concorrono sensibilmente al raggiungimento dei livelli qualitativi complessivi del servizio RUPAR, così come esso è percepito dall'utente.

B.3.1 Servizi previsti

Sono previsti i seguenti servizi:

Help Desk, finalizzato al supporto dell'utenza finale a fronte di problemi o necessità di aiuto
Gestione Dati, finalizzato alla corretta gestione dei dati dal punto di vista della garanzia di integrità a fronte di guasti e/o eventi disastrosi
Monitoraggio, finalizzato alla sorveglianza dei servizi erogati, al fine di poter intervenire in modo tempestivo al manifestarsi dei problemi, prima che a darne notizia sia l'utente finale
Registrazione attività ed eventi, finalizzato alla raccolta e all'archiviazione delle informazioni relative all'attività svolta sulla rete da parte dell'utenza

Ognuno dei servizi descritti deve essere sviluppato dai FSR così come descritto nei successivi paragrafi, con il concorso, ove previsto, del CT.

B.3.2 Modalità tecniche di erogazione dei servizi

B.3.2.1 Servizio di Help Desk

E' erogato attraverso la disponibilità dei seguenti strumenti di interazione resi disponibili all'utenza finale:

- un numero verde telefonico
- un numero verde di fax
- un indirizzo di posta elettronica
- una pagina Web

Tutti i canali di interazione devono essere presidiati e devono essere gestiti dagli operatori in modo coerente con un'unica procedura di gestione delle richieste che permetta la loro elaborazione, tenendo traccia della chiamata e di alcuni attributi ad essa relativi quali: autore della richiesta, motivo della richiesta, tempo di risoluzione del problema etc.

Il formato esatto dell'archivio delle chiamate che dovrà essere così realizzato da ogni fornitore, sarà specificato dal CT, in modo che sia possibile far convergere questi dati in un'unica banca dati del CT (cfr. servizio di "Registrazione attività ed eventi").
Oltre che gli interventi richiesti dall'utente, dovranno essere gestiti dalla stessa procedura anche gli allarmi generati dal servizio di supporto di "Monitoraggio", come di seguito specificato.

Quello descritto è uno dei due flussi operativi che intercorrono tra i due servizi, il secondo flusso è rappresentato dal possibile supporto che il servizio di Monitoraggio può fornire al servizio di Help Desk in un'analisi in tempo reale dei problemi segnalati dall'utente.

Agli utenti che attivano una segnalazione di un problema deve essere rilasciato un identificativo della segnalazione (*trouble ticket*) che gli consenta di tracciare l'evoluzione della soluzione del problema accedendo nuovamente al servizio stesso.

Inoltre, poichè alcuni malfunzionamenti possono concernere proprio l'accesso alla rete, lo stesso servizio deve essere disponibile anche via telefonica.

Le informazioni della procedura di Help Desk saranno oggetto di trasferimento verso il CT (Servizio di Registrazione attività ed eventi) per consentire elaborazioni statistiche della qualità di servizio complessiva della RUPAR.

B.3.2.2 Servizio di Gestione Dati

E' erogato per mezzo di procedure e strumentazioni idonee a realizzare copie di salvataggio dei dati dell'Amministrazione che garantiscano che i dati non vadano persi a fronte di guasti hardware delle apparecchiature che gestiscono il servizio.

In questo contesto si intende per servizio un servizio di interoperabilità, dato che le problematiche che concernono i servizi applicativi, pur essendo simili, sono di competenza dei relativi fornitori.

Si distingue tra il guasto di una singola componente (p. es. disco), a fronte del quale l'integrità dei dati deve essere totale, e il disastro (p. es. incendio) che distrugga l'intero complesso di attrezzature per mezzo delle quali un servizio viene erogato per la specifica Amministrazione.
Per questo secondo caso (problematica di *Disaster Recovery*), si definiscono i seguenti tre livelli di servizio:

- Alta criticità: si richiede che l'integrità dei dati sia garantita totalmente (schema di duplicazione dei dati in *Real Time* o in *Near Real Time*, con remotizzazione fisica dei due siti di allocazione dei dati)

- Media criticità: si accetta la perdita di dati fino ad un tempo massimo di un giorno (schema di backup giornaliero dei dati, con remotizzazione fisica del sito di allocazione del backup rispetto a quello di esercizio)
- Bassa criticità: si accetta la perdita di dati fino ad un tempo massimo di una settimana (schema di backup settimanale dei dati, con remotizzazione fisica del sito di allocazione del backup rispetto a quello di esercizio)

B.3.2.3 Servizio di Monitoraggio

Si basa sul servizio di interoperabilità di "Gestione Sistemi e Rete", del quale sfrutta l'infrastruttura tecnologica al fine di garantire la complessiva Qualità di servizio per tutti i servizi offerti da uno specifico Fornitore.

E' erogato per mezzo di operatori che sorvegliano l'andamento dei servizi intervenendo in tempo reale a risolvere problemi che eventualmente vengano segnalati dai sistemi di gestione e/o dall'Help Desk.
Parimenti gli operatori del Servizio di Monitoraggio accedono al Servizio di Help Desk per aprire, a fini rendicontativi, incidenti rilevati per mezzo dei sistemi di gestione.

Il servizio deve disporre di due canali di accesso (telefonico e posta elettronica), ignoti all'utenza e riservati all'interazione con gli analoghi servizi degli altri Fornitori e con il CT.

B.3.2.4 Servizio di Registrazione Attività ed Eventi

Il Servizio ha il compito di archiviare e trasferire verso il CT il log delle attività e degli eventi dei principali servizi di interoperabilità: Posta Elettronica, Accesso a WWW e Sicurezza (funzione Firewall), nonché del servizio di supporto Help Desk.

Il formato di ogni singolo record di registrazione e le modalità di trasferimento (temporizzazione, protocolli etc.) saranno specificati dal CT al momento della attivazione esecutiva della rete. In ogni caso tutti record del log dovranno contenere un riferimento temporale derivato direttamente dal servizio di Tempo Ufficiale di Rete.

Per quanto concerne il servizio di trasporto non è previsto che si avvalga di questo servizio di supporto, dato che le informazioni relative alla attività e agli eventi saranno gestiste direttamente dal CT mediante il proprio servizio di Gestione Sistemi e Rete via SNMP.

Lo scopo della costituzione presso il CT di una banca dati complessiva dell'utilizzazione dei servizi sulla RUPAR ha eminentemente scopi statistici e di pianificazione, consentendo uno studio di monitoraggio approfondito nel tempo dell'utilizzo degli stessi da parte dell'utente finale.

Ogni responsabilità riguardo alla riservatezza dei dati comunicati al CT da parte del Fornitore rimane in capo al CT esattamente come in capo al Fornitore ognuno per la parte di propria competenza.

B.3.3 Qualità di servizio

B.3.3.1 Servizio di Help Desk

Fascia oraria del presidio: h: 08:00-20:00 di tutti i giorni feriali
Tempo massimo di presa in carico da parte di un operatore della segnalazione via telefonica, nella fascia oraria prevista per il presidio: 30 sec.
Tempo massimo di presa in carico da parte di un operatore della segnalazione effettuata con altro canale, nella fascia oraria prevista per il presidio: 5 min.
Tempo massimo di inserimento nella base dati del tempo previsto per la soluzione del problema: 15 min.
Tempo massimo di soluzione del problema: 4 ore per problemi che bloccano l'operatività dell'utente, 2 giorni per problemi che non blocchino l'operatività dell'utente

I valori temporali indicati non devono essere superati dal fornitore nel 90% dei casi.

B.3.3.2 Servizio di Gestione dei dati

Per ognuno dei servizi di interoperabilità, cui sia applicabile la tematica di gestione dei dati sono definiti i relativi livelli di criticità:

- Gestione dei nomi: alta
- Posta Elettronica: media
- Directory: media
- Informazioni di configurazione relative agli altri servizi: bassa

B.3.3.3 Servizio di monitoraggio

Fascia oraria del presidio: h: 08:00-20:00 di tutti i giorni feriali
Tempo massimo di presa in carico da parte di un operatore della segnalazione via telefonica, nella fascia oraria prevista per il presidio: 30 sec.
Tempo massimo di presa in carico da parte di un operatore della segnalazione effettuata con altro canale, nella fascia oraria prevista per il presidio: 5 min.
Tempo massimo di inserimento nella base dati del tempo previsto per la soluzione del problema: 15 min.

Tempo massimo di soluzione del problema: 4 ore per problemi che bloccano l'operatività dell'utente, 2 giorni per problemi che non blocchino l'operatività dell'utente

I valori temporali indicati non devono essere superati dal fornitore nel 90% dei casi.

B.3.3.4 Servizio di Registrazione attività ed eventi

Il parametro principale di qualità è quello di scostamento al massimo dello 1% dei valori registrati e comunicati al CT rispetto a quelli effettivamente avvenuti, come rilevabili a posteriori mediante incrocio dei dati e/o attività di *audit*.
Si richiede altresì che la temporizzazione di trasferimento dei dati verso il CT sia rispettata con scostamenti massimi del 10%.

I dati registrati localmente vanno gestiti mediante il Servizio di Gestione Dati con criticità bassa. La durata dell'archiviazione in linea non è superiore a 12 mesi.

C I Servizi ad alto valore aggiunto e le prospettive evolutive

C.1 Relazioni con i servizi applicativi

C.1.1 I servizi applicativi sulla Rupar

E' stato già detto che i servizi di applicativi si basano sui servizi di trasporto e di interoperabilità.

Per essere più precisi essi verranno erogati mediante elaboratori posti sulla reti DMZ o RSR (in dipendenza dell'utenza target dei loro servizi) delle Amministrazioni.
Ognuno di questi host applicativi dovrà essere gestito da un unico Fornitore di Servizi Applicativi (FSA) che, qualora non coincida con il FSR che gestisce quell'Amministrazione, in buona sostanza si collegherà sulla rete DMZ o RSR con le modalità tipiche di un collegamento in "*housing*" attualmente offerto dagli ISP (Internet Service Provider) ai fornitori di soluzioni applicative; in quest'ultimo caso il fornitore del servizio di housing è il FSR che serve l'Amministrazione.

Il fatto che l'elaboratore su cui la soluzione applicativa è ospitata sia sotto il controllo esclusivo dello FSA garantisce gli attori in gioco (FSR, FSA e Amministrazione) circa la possibilità di individuare con chiarezza i confini di responsabilità reciproca per quanto attiene sia le prestazioni dei servizi che la sicurezza.

Per quanto concerne le prestazioni sarà responsabilità dello FSA garantirne i valori previsti in sede contrattuale sia in un contesto di *benchmark*, indipendente dagli altri servizi, sia in un contesto di esercizio con gli altri servizi perfettamente funzionanti, cioè a loro volta conformi ai propri dati di targa.

Per quanto concerne la sicurezza, stante il fatto che le prescrizioni obbligatorie per la sicurezza, emanate dai competenti organismi tecnici e dal CT, si applicano a tutti i livelli:

- **fisico**: responsabilità dell'Amministrazione nel caso di DMZ e RSR allocate presso di essa (nella PdR), altrimenti responsabilità dello FSR che offre il servizio di housing
- **rete**: responsabilità dello FSR
- **firewall**: responsabilità dello FSR
- **host servizio**: responsabilità dello FSA

L'Amministrazione ed ognuno dei fornitori sarà responsabile della corretta applicazione delle prescrizioni di sicurezza per la parte di propria competenza.

C.1.2 Requisiti specifici per la cooperazione applicativa

Il CT svolge anche (come previsto dai Complementi di Programmazione del POR, Asse VI, Misura 6.3, Sottomisura A, Azione b) la funzione di gestione dei servizi basilari di cooperazione applicativa, sulla base dei quali gli FSA potranno sviluppare le specifiche Applicazioni di cooperazione.

Queste funzionalità saranno rese disponibili dal CT in forma di specificazione tecnica prima, in modo da diffonderne la conoscenza al fine di agevolare la progettazione delle applicazioni cooperative, e in forma di componentistica software e servizi attivi sulla rete al momento dell'avvio delle prime applicazioni cooperative.

L'esigenza di queste funzionalità discende direttamente dalla constatazione che lo sviluppo di reali ed efficienti applicazioni cooperative tra gli Enti della PA, che sono una notevole quantità e hanno la necessità di instaurare una molteplicità di relazioni cooperative reciproche, non può non basarsi sulla disponibilità di funzioni centralizzate che semplifichino e rendano efficiente la gestione della rete di relazioni.

Leggendo le linee guida dello studio proposto dall'AIPA "Servizio di cooperazione applicativa basato su Eventi" (Gruppo di lavoro AIPA - Anasin, Assinform, Assintel sulla cooperazione applicativa), si constata, come affermato sul sito AIPA nella presentazione dello studio, che:

"*La rivoluzione delle tecnologie ICT consente oggi di proporre, anche nel contesto della pubblica amministrazione, il paradigma*

dell'impresa a latenza zero (zero latency enterprise). Si vorrebbe cioè poter realizzare un'amministrazione a latenza zero, nella quale l'interazione tra i sistemi informatici della PA connessi in rete, superando le classiche modalità batch, dovrebbe rendere possibile erogare i servizi richiesti praticamente in tempo reale."

Sulla base di questo studio sono stati specificati dal Centro Tecnico della RUPA nazionale, nel suo documento del 6/11/2001 "Rete nazionale – Architettura Applicativa – Linee Guida" al capitolo 4 "Servizi di Rete" (Specificazioni poi confluite negli allegati del I Avviso di Egovernment), i due principali servizi di supporto alla cooperazione applicativa che avranno una eminente caratterizzazione di supporto centralizzato:

- il **Servizio di Registry** (contenitore delle descrizioni dei servizi, delle modalità di utilizzo e dei formati dei dati di interscambio)
- il **Servizio di Comunicazione di Eventi** (sistema di diffusione automatica di eventi verso le Amministrazioni interessate)

Il Centro Tecnico della RUPAR Puglia provvederà, in armonia con le specificazioni tecniche ed operative del Centro Tecnico nazionale, a progettare, realizzare e gestire le funzionalità basilari che consentiranno l'attivazione di questo tipo di servizi di supporto alla cooperazione applicativa sulla RUPAR Puglia.

C.1.3 Qualità di servizio

In generale i parametri di valutazione della Qualità di servizio dei Servizi Applicativi sono i seguenti:

- periodo di erogazione del servizio: finestra temporale in cui il servizio è previsto attivo (p. es. 24 ore/giorno e 365 giorni/anno);
- uptime: tempo effettivo in cui il servizio è risultato attivo in un anno in percentuale al Periodo di erogazione del servizio (p. es. 361 giorni/anno totali di servizio attivo per un Periodo di erogazione come nell'esempio precedente è pari ad un Uptime del 99%);
- MTBF: Medium Time Between Failures, tempo medio che intercorre tra due arresti del servizio dovuti a malfunzionamenti (p. es. 1000 ore);
- tempo di ripristino, tempo necessario per il ripristino del servizio dopo una interruzione per malfunzionamento (p. es. 4 ore);
- tempo di risposta, tempo che intercorre per un utente del servizio, per ottenere risposta ad una sollecitazione inviata (p. es. 30 sec.);
- numero massimo di sessioni simultanee, numero massimo di sessioni simultanee sopportabili rispettando per ognuna di esse il precedente parametro del tempo di risposta (p. es. 1000).

Non è possibile in questa sede specificare alcun valore, che evidentemente dipende dal servizio stesso e dai requisiti qualitativi dell'Amministrazione committente, ma è possibile affermare il seguente principio generale: la valutazione a consuntivo dei parametri dovrà essere fatta al netto di eventuali scostamenti causati da malfunzionamenti degli altri servizi.

Di conseguenza interruzioni del Servizio di Trasporto o, per esempio, del servizio di interoperabilità di Gestione dei Nomi, dovranno essere tenute in conto, sottraendone la durata al Periodo di erogazione del servizio applicativo, nel calcolo dell'*Uptime* del Servizio applicativo.

Questo perchè la non accessibilità del Servizio applicativo non può, nel caso in esempio, essere ascritta al gestore dello stesso.

C.2 Politiche di sicurezza e identificazione

La rete RUPAR dovrà garantire nel suo complesso gli Enti pubblici regionali di poter interoperare a livello di Pubblica Amministrazione e di poter offrire servizi al cittadino in modo assolutamente sicuro.

Dato nell'ambito la RUPAR, per quanto descritto finora, operano una pluralità di fornitori che operano a diversi livelli (trasporto, interoperabilità di base ed applicativa), sotto il coordinamento ed il controllo del CT, è evidente che la problematica della sicurezza investe l'attività di tutti questi soggetti che sono responsabili, ognuno per la propria parte, della complessiva attuazione delle necessarie politiche di sicurezza.

Si deve sottolineare con forza che il tema della sicurezza è, prima che un tema strettamente tecnico, un tema di tipo funzionale ed organizzativo, in quanto sono cruciali sia l'individuazione precisa delle aree soggette ad una problematica di sicurezza sia la catena di responsabilità dei soggetti preposti a garantirla.

E' proprio in questa constatazione uno dei punti di forza dell'idea di realizzare una **rete unitaria della PAL**, senza limitarsi ad ipotizzare che le stesse Amministrazioni interoperino direttamente mediante la rete Internet, dato che solo una rete gestita e controllata in modo unitario può dare le **garanzie funzionali** ed **organizzative** di cui si è parlato.

Questa considerazione è vera anche nel caso del modello cosiddetto "aperto" che si è ritenuto di adottare nella realizzazione della RUPAR della Regione Puglia, in cui appunto i fornitori sono molteplici ed ovviamente sono soggetti che operano anche sul generico mercato di Internet.

Il processo di qualificazione dei fornitori della RUPAR, la loro sottoscrizione di precisi standard contrattuali di servizio e relativi **SLA** (*Service Level Agreement*), la loro accettazione del ruolo di supervisione del CT nel controllo e nella gestione della RUPAR, ovviamente anche nel campo della sicurezza, sono gli elementi che conferiscono valore aggiunto alla soluzione di una rete Extranet (la RUPAR appunto) dedicata alla PAL, in luogo della semplice interoperabilità su Internet.
Da questa impostazione, che porta a collocare in un contesto definito e chiaro i soggetti interessati, discende la possibilità di definire con chiarezza la catena di responsabilità relativa alla sicurezza, come illustrata nei successivi paragrafi.

Per quanto concerne l'importante tema dell'identificazione degli utenti che operano su RUPAR, problema fortemente correlato a quello dei diritti di accesso alle informazioni ed alle funzioni, si ritiene che esso debba essere affrontato a più livelli.

Un primo livello è quello dell'identificazione semplice, basata sui normali meccanismi di "Username" e "Password" (comunque eseguiti sotto la protezione crittografica del protocollo **SSL**), che permetta di autenticare in modo semplice e "leggero" gli utenti ai fini di accesso a servizi non critici, per i quali si intenda comunque mantenere traccia di chi accede eventualmente a fini meramente statistici.

Un secondo livello è quello dell'identificazione forte, basata su meccanismi di **Infrastruttura a Chiave Pubblica** (**PKI**), destinata a garantire l'accesso a servizi con elevati requisiti di restrizione dell'accesso.
La differenza sostanziale tra i due livelli è data dal fatto che nel primo caso l'identificazione del soggetto si basa unicamente sulla sua conoscenza di un'informazione riservata (la "password"), che potrebbe essere carpita all'interessato ed usata a sua insaputa, mentre nel secondo caso l'identificazione si basa sia sulla conoscenza di un'informazione analoga (PIN code) che sul possesso di un oggetto fisico (la Smart Card).

Il secondo livello di autenticazione a "due fattori", analogo a quello che si ha per le tessere Bancomat e/o telefoniche, ha una maggiore robustezza intrinseca in quanto comporta la necessità di impadronirsi di entrambi i fattori (PIN Code e Smart Card) per poter effettuare un'identificazione falsa.
Per contro il secondo livello richiede una maggior complessità organizzativa (recapito e gestione delle Smart Card) e tecnolo-

gica (disponibilità sui Personal Computer degli utenti di periferiche di lettura delle Smart Card).

Si prevede che entrambi i livelli debbano essere supportati da servizi centralizzati gestiti dal Centro Tecnico nell'ambito delle sue funzioni di supporto alla cooperazione applicativa, nella filosofia comunemente denominata "***Single SignOn***".

Secondo questa impostazione è corretto che un utente di un insieme di servizi offerti su una rete non sia continuamente sottoposto a richieste di autenticazione da parte di ogni singolo servizio a cui accede, ma si autentichi una volta per tutte (autenticazione di rete) la prima volta che questa operazione è necessaria, tipicamente al momento dell'accesso alla RUPAR, e nelle successive interazioni del stessa sessione di lavoro i servizi acceduti prendano automaticamente atto dell'avvenuta autenticazione.

Questo tipo di soluzione, che si prevede di adottare essenzialmente per gli utenti "interni" della RUPAR, ha alcuni grossi vantaggi:

- semplifica la navigazione in rete dell'utente
- semplifica lo sviluppo delle applicazioni e la loro cooperazione, offrendo loro un *framework* adeguato per la gestione dell'utenza
- rende disponibile una base dati congruente degli utenti dei servizi della rete

La soluzione si baserà sul servizio "***Directory***" di interoperabilità di base, che per definizione conterrà l'intera descrizione della struttura organizzativa del personale delle pubbliche amministrazioni della regione, completa di informazioni di utilità quale il numero di telefono e l'indirizzo di Email individuale.

Questa descrizione complessiva discende dall'unione delle singole basi dati di Directory gestite dai diversi fornitori come previsto dalle funzionalità LDAP.
Gli sviluppatori di applicazioni su RUPAR potranno avvalersi di queste funzionalità per integrare in modo ottimale la propria applicazione nel contesto RUPAR.

C.2.1 Sicurezza dei dati e delle funzioni

Come detto nel paragrafo precedente la chiave di volta della corretta attuazione di una politica di sicurezza sta nella individuazione attenta della catena di responsabilità.
Nel caso della RUPAR gli elementi di questa catena sono i seguenti:

- l'Amministrazione Pubblica utente del servizio RUPAR
- il Fornitore del Servizio RUPAR (FSR)
- il Fornitore del Servizio Applicativo (FSA)
- il Centro Tecnico

Si può schematicamente riassumere nelle seguenti definizioni quanto compete ad ognuno dei precedenti soggetti riguardo alla tematica della sicurezza:

L'Amministrazione Pubblica individua il livello di criticità delle informazioni da essa gestite che devono essere oggetto di cooperazione su RUPAR; definisce i criteri di protezione ed i profili dei diritti di accesso alle funzioni da parte degli utenti.

Il FSR mette in pratica le raccomandazioni generali di sicurezza prescritte dal CT per la protezione delle reti di servizio, personalizzandole al caso specifico sulla base dei criteri e dei profili definiti dall'Amministrazione; questa attività concerne i servizi di interoperabilità di base e la gestione del Firewall.

Il FSA mette in pratica le raccomandazioni generali di sicurezza prescritte dal CT per la protezione degli elaboratori di servizio, personalizzandole al caso specifico sulla base dei criteri e dei profili definiti dall'Amministrazione; questa attività concerne l'intero ambiente hardware e software preposto all'erogazione: Sistema Operativo, eventuali Middleware e l'Applicazione stessa.

Il FSR mette in pratica le raccomandazioni generali di sicurezza prescritte dal CT per la protezione del traffico di rete, personalizzandole al caso specifico sulla base dei criteri e dei profili definiti dall'Amministrazione.
IL CT prescrive le politiche generali di sicurezza, effettua attività di auditing periodico nei confronti dei Fornitori ivi compresi test di impenetrabilità, supporta l'Amministrazione nella definizione delle problematiche di sicurezza e nell'interazione con i Fornitori in caso della rilevazione di problemi.

C.2.2 Riservatezza delle informazioni (Privacy)

La problematica della riservatezza dei dati personali (Privacy), come regolamentata delle disposizioni legislative Legge 675/96 e DPR 318/99, è di pertinenza di ognuno dei soggetti precedentemente elencati per i dati da essi legalmente detenuti.

Questo significa che le Amministrazioni saranno responsabili dei dati personali, tipicamente dei cittadini, gestiti dalle applicazioni attivate sotto la propria responsabilità sulla RUPAR, mentre i fornitori saranno responsabili eventualmente dei dati personali che dovessero raccogliere nell'ambito della propria attività di gestione del servizio.

La definizione di responsabilità della gestione di un insieme di dati personali è fatta nel senso delle disposizioni legislative precedentemente richiamate e comporta l'obbligo di nominare un titolare del trattamento dei dati e un responsabile del trattamento dei dati, quest'ultimo ha a sua volta l'obbligo di predisporre un piano di sicurezza.
Nel caso tipico in cui il responsabile del trattamento opera per conto di un'Amministrazione, i Fornitori in ambito RUPAR (FSA e FSR), assolvono al ruolo di esecutori delle disposizioni del piano, riferiti nella normativa come "Amministratori di Sistema", assumendosi la responsabilità della loro corretta esecuzione.

Il CT provvederà a diffondere le regole generali di attuazione dei piani di sicurezza relativi al trattamento dei dati personali e includerà la loro attuazione tra le attività che saranno garantite dai fornitori, all'interno del Service Level Agreement (SLA), incluse nel canone del servizio.

C.2.3 Infrastruttura a chiave pubblica e "Firma Digitale"

Si definisce in generale "**Infrastruttura a Chiave Pubblica**" o **PKI** (**P**ublic **K**ey **I**nfrastructure) un ambiente hardware e software in grado di identificare individui ed oggetti (applicazioni/servizi), basandosi sul meccanismo delle doppie chiavi crittografiche (pubblica e privata).

Questi ambienti si prestano in generale ad una identificazione caratterizzata da una elevata certezza e sicurezza, raggiungendo una sicurezza che si può presumere assoluta quando sono realizzati e gestite secondo le più rigorose norme organizzative e funzionali.

Questo è il caso delle cosiddette "Firme digitali" che altro non sono che oggetti software (certificati), facenti parte di PKI gestite da organizzazioni (le "Autorità di Certificazione"), che hanno conseguito presso l'AIPA l'omologazione, concessa sulla base del rispetto di rigorosi standard organizzativi, funzionali e tecnici, per poter gestire questi oggetti aventi valore legale di firma, come previsto dalla Legge n. 59 del 15/3/1997 e successivi DPR 513/97 e DPCM 8/2/99.

Come già illustrato nel primo paragrafo, la RUPAR renderà disponibili meccanismi di "***Strong Authentication***" basati su PKI fornendo un servizio centralizzato che consenta alle Applicazioni su RUPAR, caratterizzate da stringenti requisiti di controllo dell'accesso, di avvalersi di funzionalità condivise in rete che ottimizzano sia il carico sull'utente che la gestione delle informazioni di accesso in rete.

Un'estensione molto importante di questa funzionalità è quella costituita dalla Firma Digitale propriamente detta che riveste un ruolo estremamente importante nell'ambito della cooperazione applicativa tra le Pubbliche Amministrazioni.

Va notato infatti che la cooperazione tra Amministrazioni presuppone un consistente scambio di informazioni tra di esse, scambio che, per essere effettuato con il rispetto delle regole per i procedimenti inter-amministrativi, necessita di essere firmato da chi ha la responsabilità delle informazioni e del loro trasferimento ad altra Amministrazione.

Nel momento in cui questo scambio, per diventare più efficiente, viene effettuato in modalità elettronica anziché cartacea, sorge la necessità di poter firmare in modo legalmente valido il trasferimento elettronico di informazioni.

Si fa notare che la più semplice modalità di scambio di informazioni in formato elettronico è la Posta Elettronica che, essendo un servizio di interoperabilità di base, sarà immediatamente disponibile all'avvio della RUPAR anche in assenza di specifiche applicazioni cooperative, le quali presumibilmente seguiranno dopo un certo lasso di tempo dall'avvio della rete.

Per poter essere effettivamente utile nello snellimento di iter procedurali inter-amministrativi, la Posta Elettronica necessita di essere integrata dalla Firma Digitale, come sottolineato nella seguente citazione dal documento AIPA "Linee guida alla realizzazione dei sistemi di protocollo informatico e gestione dei flussi documentali nelle pubbliche amministrazioni" ("Gedoc2", par. 5.7.2 "Comunicazione inter-amministrazione", pag.42):

"*Sia nel caso di gestione assistita da un workflow che in casi meno strutturati, appare come fondamentale l'utilizzo della posta elettronica e della tecnologia della firma digitale per trasmettere documenti in modo sicuro con validità giuridica. Il DPR 428 e le relative regole tecniche prevedono, a tal fine, specifiche indicazioni e riferimenti al caso in cui il documento da protocollare in uscita sia formato e trasmesso con strumenti informatici. In tal caso si prevede che la "segnatura di protocollo" possa comprendere tutte le informazioni che vengono gestite dal sistema di protocollo dell'amministrazione che forma il documento. Si tratta di un meccanismo che consente di inviare con il medesimo messaggio, oltre al documento in senso stretto, anche un insieme di informazioni strutturate (la segnatura) che, se riconosciute dal destinatario, potrebbero essere utilizzate per velocizzare i processi di ricezione della corrispondenza e, conseguentemente, i processi di servizio ad essi collegati.* "

Ne consegue che la RUPAR non può prescindere, sin dal suo avvio, dalla disponibilità di servizi di Firma Digitale, che possono consentire alle Pubbliche Amministrazioni locali di avviare rapidamente interscambi di informazioni più efficienti, che rappresentano eventualmente esclusivamente l'automazione elettronica di un interscambio già operativo in forma cartacea.

Dato che però il rilascio di certificati di Firma Digitale a validità legale è consentito solo alle CA omologate da AIPA e che assumere il ruolo di CA omologata ha dei costi che possono essere compensati solo nel caso in cui si operi su un volume potenzialmente elevato di utenti, si ritiene che la soluzione migliore sia quella, in perfetta coerenza con il modello "Aperto" scelto per i servizi di Trasporto ed Interoperabilità, di far erogare questo servizio sulla RUPAR da una pluralità di CA omologate che si uniformeranno a specifici requisiti funzionali ed economici.

C.2.4 Standard tecnici di riferimento

Per quanto concerne l'approccio metodologico alla problematica della sicurezza dei Sistemi Informatici uno standard di riferimento è l'ITSEC, emanato da agenzie governative del Regno Unito, Germania, Francia e Olanda.

La successiva armonizzazione di questo standard con analoghi standard elaborati in Nord America (USA e Canada) ha portato alla ratifica della versione 2.0 di ITSEC come ISO 15408; l'ISO ha successivamente emanato, nella stessa area, lo standard ISO17799.

In Italia un importante riferimento è il documento “LINEE GUIDA PER LA DEFINIZIONE DI UN PIANO PER LA SICUREZZA DEI SISTEMI INFORMATIVI AUTOMATIZZATI NELLA PUBBLICA AMMINISTRAZIONE” del Gruppo di Lavoro AIPA-ANASIN-ASSINFORM-ASSINTEL, disponibile sul sito AIPA**.**

Per quanto concerne la sicurezza sulla rete Internet gli standard di riferimento sono gli RFC2401 (IPSec) e RFC2196 (Site Security Handbook).

Gli standard relative alla Firma Digitale sono:

- Per i formati di codifica, certificazione ed imbustamento delle firme: PKCS#1 (RSA), X.509 ed il PKCS#7 ver 1.5 (RFC 2315).
- Per i formati accettabili: ASN.1-DER (ISO 8824, 8825), BASE64 (RFC 1421) e PKCS#7 (RFC 2315).
- Per la generale definizione della PKI: RFC 2459 “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”.

C.3 Prospettive evolutive

La Rete Unitaria delle Pubbliche Amministrazioni della Regione Puglia rappresenta lo strumento attraverso il quale un qualunque utente autorizzato può accedere ai dati dei sistemi informativi delle Pubbliche Amministrazioni.

La RUPAR Puglia, come già descritto, prevede attraverso una armonica cooperazione federata di fornitori di servizi il raggiungimento dei seguenti obiettivi:

- creare un'architettura idonea alla cooperazione applicativa;
- fornire un primo bouquet di servizi di interoperabilità;
- adeguare costantemente le soluzioni all'evoluzione tecnologica ed alle migliori condizioni economiche di mercato.

A differenza dei primi due punti che sono stati ampiamente descritti nei paragrafi precedenti, il presente paragrafo intende analizzare l'argomento "evoluzioni" finalizzato a:

- migliorare i servizi attualmente disponibili;
- rendere economicamente più vantaggiosa la fruizione dei servizi;
- aumentare l'offerta di servizi qualificati e trainanti derivandoli dal mondo dell'Information e Communication Technology.

C.3.1 Gestione dei cambiamenti

L'analisi dei livelli di servizio, del rapporto con il cliente/utente, dei trend tecnologici permetterà ai soggetti attuatori di RUPAR

Puglia di individuare e prevenire situazioni di criticità. Tale monitoraggio permetterà, anche in funzione del numero di Domini Amministrativi che si prevede popoleranno la RUPAR nel tempo, di adeguare gli impianti, le piattaforme e le procedure di erogazione dei servizi all'utenza.
In generale, attraverso l'azione congiunta del Centro Tecnico, dei Centri di Gestione, dei Fornitori di servizi applicativi verrà garantita l'evoluzione dei prodotti e dei servizi mediante:

- la rimozione di difetti dall'esistente;
- l'introduzione di nuove versioni di prodotti già utilizzati;
- l'introduzione di nuove soluzioni individuate.

Il controllo ed il monitoraggio continuo consentirà alla RUPAR di mantenere adeguati livelli di servizio, permetterà lo sviluppo di nuovi servizi e quindi di nuove opportunità di mercato per tutti gli operatori.

C.3.2 Nuovi servizi

L'osservazione di fenomeni legati al mondo dall'IT unita alla sensibilità dei Soggetti attuatori della RUPAR nel cogliere e recepire i fabbisogni della P.A. dovrà essere il filo conduttore per innovare la rete unitaria regionale pugliese.

Il rapporto con l'utenza permetterà, attraverso previsioni di efficacia delle nuove soluzioni tecniche e tecnologiche standard di

mercato, di completare/migliorare il portafoglio servizi.

La conoscenza del mercato e dei trend tecnologici permette già di ipotizzare un orizzonte fatto di applicazioni multimedia, di telefono, di radio e di televisione sempre più integrati alle tecnologie Internet ed in generale di applicazioni sempre più *real-time*.

Una prima lista di servizi che potranno essere resi disponibili sulla infrastruttura di comunicazione della RUPAR-Puglia è la seguente:

- Telefonia (VoIP, Voice Over Ip)
- Audio e video conferenza e multi videoconferenza
- Digital Video Broadcasting

Tutti i fornitori di servizi abilitati della rete RUPAR dovranno impegnarsi a garantire/supportare i servizi di cui sopra; inoltre, i fornitori aderiranno al supporto di nuovi servizi che il Centro Tecnico dovesse loro richiedere.

C.3.3 Adozione di nuove tecnologie

La fruizione di nuovi servizi applicativi, come quelli *real-time* elencati precedentemente, non può essere gestita con il protocollo IP classico. Per una adeguata gestione dei servizi *real-time*, è necessaria una gestione quantitativa e qualitativa del traffico di

rete, occorre disporre di elementi di riconoscimento e di gestione dei *requirements* delle applicazioni per trattare quelle particolarmente esigenti in maniera diversa dalle altre.

Contemporaneamente, sono anche necessari meccanismi in grado di classificare i pacchetti che possono subire ritardi di trasmissione rispetto a quelli che non tollerano alcun ritardo.
In definitiva, come per le infrastrutture di rete IP, anche per la RUPAR si manifesta la necessità di richiedere garanzie di *delivery* alla rete di trasporto mediante l'introduzione di tecnologie che permettano la gestione della QoS (Quality of Services).

I fornitori RUPAR dovranno cooperare in modo da garantire sull'intera RUPAR la fruizione di servizi *QoS-enabled* a tutti i Domini Amministrativi.
Essi si adopereranno per supportare i seguenti algoritmi/protocolli:

- Multi Protocol Label Switching (MPLS)
- ReSerVation Protocol (RSVP)
- Differentiated Services (DiffServ)

Inoltre, i fornitori RUPAR si impegneranno a supportare future evoluzioni del protocollo IP, già noto come IPv6, protocollo già progettato per un supporto *bundle* della QoS.

D Attivazione e esercizio

D.1 Dimensionamento

Il presente capitolo contiene delle previsioni di massima relativamente al dimensionamento ed ai costi della RUPAR, i valori indicati potranno non corrispondere esattamente a quelli che saranno determinati successivamente nel corso delle procedure di affidamento ed attivazione dei servizi.

D.1.1 Pianificazione quantitativa degli Enti da servire

La finalità della RUPAR è l'interconnessione della Pubblica Amministrazione Locale (PAL) della Puglia.

Nella scelta degli Enti da collegare nel periodo di gestione della rete mediante il sostegno del POR, saranno considerati in modo speciale, oltre alle principali amministrazioni (Regione, Province, Comuni etc.), gli Enti che siano collegati o riconducibili alle principali azioni di informatizzazione previste dal POR, al fine di rendere concreta e vicina l'attivazione di servizi ad alto valore aggiunto nella PAL.

Con questa convenzione la seguente tabella mostra l'utenza potenziale che la RUPAR deve servire, il totale di **350** è il numero indicato come obiettivo nei Complementi di Programmazione del POR:

Amministrazione	**Quantità**	**Asse**
Regione	1	Tutti
Provincia	5	Tutti
Comune	258	Tutti
Comunità montana	6	Tutti
Azienda sanitaria (ASL)	12	VI
Area Sviluppo Industriale (ASI)	5	V
Agenzia regionale per il lavoro	1	III
Consorzio di Bonifica	6	III
Agenzia Regionale Protezione dell'Ambiente	1	I
Enti Parco	2	I
Altri Enti	53	
TOTALE	**350**	

Tabella D-1

Nel successivo capitolo sulla previsione dei costi è riportata la pianificazione della previsione di spesa che discende dalla pianificazione globale del budget della Misura 6.3 del POR.
Questa pianificazione costituisce il vincolo di spesa che deve guidare la pianificazione delle attivazioni dell'utenza, ma si possono al riguardo fare le seguenti considerazioni:

- in virtù della scelta fatta di realizzare la RUPAR mediante l'erogazione di un servizio di comunicazione da parte di fornitori qualificati del settore, anziché mediante una infrastruttura interamente di proprietà regionale, gli investimenti previsti sono minimi (essenzialmente l'attivazione tecnologica del CT);

- la scelta di adottare il modello aperto ha come conseguenza che l'utenza da servire potrà essere connessa in rete ad opera di una pluralità di fornitori in concorrenza tra di loro e quindi con un processo sostanzialmente di elevato parallelismo, senza possibili ritardi dovuti allo svolgimento in sequenza delle attività da parte di un unico fornitore;
- il costo annuo, dovuto essenzialmente ai canoni del servizio, tenderà ad essere costante una volta connessa l'utenza, per cui è sufficiente che la pianificazione dei costi consenta costi crescenti per tutto il periodo di attivazioni di nuova utenza (setup della rete) e costi costanti per il periodo successivo.

Sulla scorta di queste considerazioni, e coerentemente con gli indicatori di risultato comunicati dalla Regione Puglia alla Comunità Europea ed ai competenti Ministeri nazionali, si è previsto il ***trend*** di crescita del numero degli Enti collegati in RUPAR, mostrato nella seguente Figura:

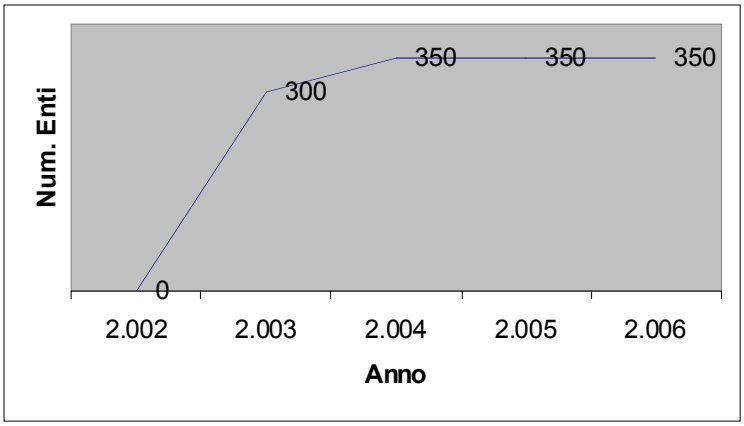


Figura D-1

Questo trend si basa sulla constatazione che non sarà possibile attivare utenza nel corso del 2002, anno che è stato destinato all'espletamento delle attività di progettazione, affidamento e realizzazione della RUPAR, e che si prevede di poter collegare la totalità degli Enti già individuati in Tabella D-1 nel corso del primo anno (2003).

Gli ultimi tre anni (2004-2006) saranno quelli in cui si dovrà raggiungere l'obiettivo di attivare il più un ampio spettro possibile di servizi applicativi, che in definitiva sono il principale valore aggiunto dell'iniziativa.

L'attivazione compiuta di un elevato numero di servizi applicativi che effettivamente incrementino l'efficienza della Pubblica Amministrazione nel suo complesso, è la maggiore garanzia che l'iniziativa RUPAR continui ad essere alla base dell'attività della

PAL anche negli anni successivi, una volta terminato dell'intervento di sostegno assicurato dai POR.

Dal punto di vista della pianificazione temporale delle attivazione, si prevede comunque di adottare un criterio di maggiore urgenza per le PAL di maggior dimensione e ruolo funzionale (Regione, Province, Capoluoghi di provincia, grandi comuni) e di dipendenza funzionale da servizi applicativi la cui attivazione è prevista in tempi brevi.

D.1.2 Previsione qualitativa dei servizi per tipologia di Ente

Per definire i servizi che si prevede di attivare per l'utenza vanno preliminarmente fatte le seguenti considerazioni:

- a servizi qualitativamente migliori corrispondono costi maggiori
- la scelta del miglior rapporto costo/prestazioni è normalmente di competenza dell'utente finale che stipula il contratto e che ne sopporta gli oneri
- nel quadro dell'avvio della RUPAR con il sostegno finanziario della Comunità Europea per mezzo dei POR, la determinazione di questo rapporto non può essere fatta dalla Regione Puglia che gestisce l'iniziativa in modo puntuale per ogni singola utenza da collegare

Ne consegue quindi l'opportunità di individuare fasce qualitative di servizio, sia per i servizi di trasporto che di interoperabilità, ed attribuirle alle diverse tipologie di Amministrazioni da collegare, valutando infine la compatibilità finanziaria rispetto alla copertura fornita dal POR.

A questo fine si indicano nel seguito le fasce qualitative dei servizi, illustrandone la principale caratteristica che le qualifica rispetto alle altre.

D.1.2.1 Servizi di trasporto

I Servizi di Trasporto sono caratterizzati da una molteplicità di possibili tipi di collegamenti e soprattutto di possibili velocità del collegamento, che ne costituisce il parametro fondamentale dal punto di vista qualitativo.
Ogni velocità di collegamento (da 64Kbps a 2Mbps) è realizzabile per mezzo di una delle seguenti tecnologie:

- CDN per tutte le velocità
- ISDN con aggregazione dei canali per velocità superiori a 64Kbps
- ADSL con diverse limitazioni della velocità di upload fino a 512Kbps
- HDSL per velocità comprese tra 512Kbps e 2 Mbps

Le diverse tecnologie utilizzabili per fornire il servizio sono caratterizzate da diversi schemi tariffari (canone o “flat”, a tempo, a volume di traffico), anche in dipendenza dei diversi fornitori e delle diverse filosofie commerciali.

Al fine di rendere ulteriormente omogenea la pianificazione, si ipotizzeranno nel seguito dei costi medi di tipo a canone (o flat) in coerenza con quanto previsto dall’Authority delle Telecomunicazioni nella sua delibera 15/00/CIR, che ha esplicitamente indicato come riferimento importante uno schema tariffario di tipo flat.

In questa ottica paritetica, i servizi di tipo commutato come lo ISDN possono essere pensati, ai fini della pianificazione, caratterizzati sia dall’uso di un numero verde, per consentire la tariffazione flat, sia dalla funzionalità di “call-back”, per rendere del tutto equivalente dal punto di vista funzionale della raggiungibilità dalla rete un collegamento ISDN (commutato) ad uno di tipo CDN o xDSL (permanente).

Sono state individuate sette velocità di riferimento per i Servizi di Trasporto, riportate nella seguente tabella:

Sigla servizio	Kbps
A	2048
B	768
C	512
D	384
E	256
F	128
G	64

Tabella D-2

Si noti che tutte le tecnologie precedentemente menzionate sono considerate nell'ipotesi che la loro vendita al pubblico sia pienamente ammessa dalla normativa vigente al momento dell'attivazione della RUPAR.

D.1.2.2 Servizi di interoperabilità

I Servizi di interoperabilità non sono caratterizzati da possibili differenze qualitative, in quanto vanno totalmente attivati così come stati definiti, variando ovviamente da un'Amministrazione all'altra il volume del servizio in dipendenza della dimensione dell'Amministrazione stessa (p. es. numero di caselle di Posta Elettronica).

Ne consegue che una previsione qualitativa dei servizi di interoperabilità verte essenzialmente sulla possibile differenziazione dell'allocazione delle due reti di erogazione servizi (DMZ e RSR).

La soluzione della loro allocazione presso un Centro Servizi del Fornitore di Interoperabilità è adeguata nella gran maggioranza dei casi e sarà quella generalmente adottata, specie per le amministrazioni più piccole.

In alcuni casi la complessità delle interazioni previste per i servizi applicativi che dovranno essere attivati nei PdR potrà consigliare l'allocazione di queste reti presso la sede dell'Amministrazione, soluzione questa che comporta sicuramente costi maggiori e che probabilmente potrà essere adottata solo per le grandi Amministrazioni.

D.1.2.3 Servizi di Firma Digitale

Ai servizi di trasporto e Interoperabilità si aggiunge un insieme iniziale di servizi di Infrastruttura a chiave pubblica (PKI) che si prevede di attivare nel contesto dell'Azione a), come predisposizione avente i seguenti due principali obiettivi:

- dotare una serie di figure istituzionali della PAL (Sindaci, Assessori, Dirigenti etc..) di una documento ufficiale di

Firma Digitale, di classe corrispondente al ruolo ricoperto, al fine di facilitare l'avvio dell'utilizzo "formale" di strumenti di interoperabilità di base come la Posta Elettronica

- facilitare l'avvio dei primi progetti applicativi per quanto concerne la gestione del problema PKI sia dal punto di vista tecnico (interoperabilità tecnologica) sia dal punto di vista economico (condivisione costi)

Il livello di servizio che si prevede di richiedere alle Società accreditate da AIPA come Certification Authority è quello di certificati individuali (per persona fisica) di Firma Digitale rilasciati su smart card.
Altre funzioni opzionali saranno quelle di fornire certificati digitali da utilizzare per la cifratura dei documenti e/o per l'autenticazione forte oppure per la certificazione dei servizi offerti sulla RUPAR e/o di fornire meccanismi di autenticazione debole "interna" in outsourcing per la gestione degli iter delle pratiche (firma elettronica).

Il servizio potrà essere erogato dalle organizzazioni accreditate come CA da AIPA che si qualificano dal punto di vista organizzativo ed economico per erogare il servizio su RUPAR Puglia.

D.1.2.4 Altri Servizi

Per una questione di ottimizzazione gestionale si ritiene opportuno allocare gli EPO presso le centrali o sedi di uno dei FSR, che offra quindi un servizio di ospitalità (*housing*) per la struttura di un EPO in ogni capoluogo di provincia.
Questa soluzione consente di evitare all'Ente Regione di dover predisporre propri locali per l'ospitalità degli EPO, con l'aggravante che le sedi della Regione Puglia sono ovviamente destinate ad uso ufficio e mal si presterebbero ad ospitare infrastrutture tecnologiche sia pure di dimensioni contenute.

Inoltre l'allocazione presso l'infrastruttura di un Fornitore di Trasporto apre interessanti prospettive di possibili sinergie di costi tra i vari Fornitori in dipendenza della possibilità che vengano coincidere siti di colocazione degli accessi a canale disaggregato (*Unbundling Local Loop*) con siti in cui viene allocato l'EPO della RUPAR.

Fa eccezione la sede dell'EPO di Bari, che si prevede di allocare presso l'infrastruttura tecnica del Centro Tecnico, che opererà presso il Parco Scientifico Tecnopolis a Valenzano, vicino Bari.

D.1.3 Criteri per la previsione dei volumi di servizio

Per i volumi di servizio da attivare si prevede di adottare come principale criterio valido, nonché sicuramente oggettivo, quello della dimensione dell'Ente in termini di Posti di Lavoro (PdL).

Sono state individuate le seguenti sette classi dimensionali significative per la tipica dimensione delle PAL:

Classe dimensionale	Numero PdL
A	> 2000
B	1000 – 2000
C	500 – 1000
D	250 – 500
E	100 – 250
F	50 – 100
G	< 50

Tabella D-3

Le diverse classi di servizio sia di Trasporto che di Interoperabilità saranno quindi attivate per ogni Ente previsto in Tabella D-1, in dipendenza della effettiva dimensione dell'Ente e della classe dimensionale in cui si iscrive secondo quanto riportato in Tabella D-3.

Ai fini della previsione del budget, data l'oggettiva difficoltà di ottenere una mappa dettagliata dei dipendenti del Enti Pubblici locali e dato che la gran maggioranza di essi è costituita dai

Comuni, si è proceduto con una stima del numero di dipendenti dei Comuni sulla base del numero degli abitanti, che è ben noto, e di alcuni tipici rapporti tra dipendenti comunali e abitanti che si riscontrano nella PAL: si va da circa 0,45 dipendenti ogni 100 abitanti per i piccoli comuni a circa 0,65 dipendenti ogni 100 abitanti per i grandi comuni.

D.1.4 Stima della dimensione della rete

La dimensione della rete può essere definita in base a diversi parametri:

- estensione delle dorsali della rete: si tratta delle linee di interconnessione tra gli EPO provinciali e l'EPO di Bari ed equivale alla somma delle distanze tra Bari e i capoluoghi di provincia, pari a circa 450 Km
- massima distanza tra due utenze della rete: si tratta della distanza tra i comuni più remoti delle province di Foggia e Lecce, pari a circa 350 Km
- numero di Enti serviti: è quello riportato in Tabella D-1, pari a circa 350 Enti

- estensione complessiva dei collegamenti della rete: si calcola partendo dalla valutazione del numero di Enti allocati fuori dai capoluoghi di provincia (circa 280), moltiplicando per una stima della distanza media dal capoluogo (40 Km), ottenendo così un valore superiore a 10.000 Km
- numero di utenti diretti serviti (PdL della PAL): circa 20.000

La rete così dimensionata è al servizio della popolazione pugliese che raggiunge i 4.000.000 di persone.

D.2 Previsione costi

La previsione dei costi è effettuata sulla base sia del costo dei singoli servizi sia della pianificazione dell'attribuzione dei servizi agli Enti in dipendenza della loro classe dimensionale prevista in Tabella D-3.

D.2.1 Stima del costo dei singoli servizi

I singoli servizi per i quali si deve prevedere una stima dei costi ai fini di pianificazione del budget sono le classi di Servizio di Trasporto previste in Tabella D-2 ed il Servizio di Interoperabilità previsto sempre nel caso più generale di erogazione presso il Centro Servizi di un FSR, dipendente però dal volume dell'utenza servita secondo le classi dimensionali previste in Tabella D-3.

La stima più precisa, di cui si dispone al momento è quella dei listini applicati per gli stessi servizi nella RUPA nazionale.

La seguente tabella riporta il canone annuo RUPA per il Servizio di Trasporto IP (BMG pari a 0,5 della velocità del collegamento) aggiornato all'ultima revisione prezzi di Gennaio 2002 e considerato nel caso di fascia geografica equivalente alla caratterizzazione più diffusa nella RUPAR-Puglia (fascia D, comuni con numero di abitanti tra 5.000 e 30.000):

Sigla servizio	Kbps	Canone annuo flat (€)
A	2048	33.940,56
B	768	22.290,84
C	512	18.096,96
D	384	15.609,00
E	256	13.093,44
F	128	8.527,32
G	64	5.774,28

Tabella D-4

Tutti i servizi si riferiscono a collegamenti IP di tipo permanente, che sono reputati in linea generale i più idonei al collegamento di una Pubblica Amministrazione.

La seguente tabella riporta il canone annuo RUPA per il Servizio di Interoperabilità, parametrato sulle classi dimensionali applicabili in RUPAR-Puglia e definite nella Tabella D-3.

Questa operazione di parametrizzazione si è resa necessaria poiché il Servizio di Interoperabilità viene fornito in RUPA a 50 grandi Amministrazioni Centrali dello Stato, la cui dimensione media è nettamente superiore a quella delle PAL pugliesi: si è così potuto calcolare in modo pesato il costo del servizio per PdL per le diverse classi dimensionali RUPA, estendendolo poi alle dimensioni minori di interesse per la RUPAR; si è tenuto conto di un'ipotesi prudenziale di traffico.

Classe dimensionale	Numero PdL	Canone annuo flat (€)
A	> 2000	228.662,00
B	1000 - 2000	163.330,00
C	500 - 1000	124.272,82
D	250 - 500	66.990,82
E	100 - 250	31.262,38
F	50 - 100	13.398,16
G	< 50	13.398,16

Tabella D-5

Per le ultime due classi (F e G) si è ritenuto che il costo vada prudenzialmente posto eguale allo stesso valore per tenere conto del fatto che un certo tipo di investimenti infrastrutturali (p. es. piattaforme di elaborazione) non può avere un valore tendente a zero anche nel caso di necessità contenute.

I valori della Tabella D-5 possono essere confrontati con il canone annuo medio RUPA per Amministrazione che vale Euro. 171.496,50.

Per il servizio di Firma Elettronica si prevede un costo medio annuo di Euro. 35 per singolo certificato individuale (completo del dispositivo di firma o smart card).

E' utile precisare che la stima dei costi dei singoli servizi di cui al presente paragrafo viene effettuata solo ai fini di determinazione del budget e deve rappresentare un estremo superiore dei costi che si avranno sulla RUPAR.

D.2.2 Valutazione dei costi complessivi

D.2.2.1 Costi dei Servizi di Trasporto e Interoperabilità

I costi complessivi dipendono dall'attribuzione dei singoli servizi alle diverse classi dimensionali di Enti; la seguente tabella mostra la distribuzione dei costi stimati servizi in funzione delle diverse classi dimensionali degli Enti da servire:

Classe	Numero PdL	Num. Enti	Velocità Trasporto (Kbps)	Costo Annuo Trasporto	Costo Annuo Interoperabilità	Costo Annuo TOTALE (€)
A	> 2000	1	2048	33.940,56	228.662,00	262.602,56
B	1000-2000	4	768	22.290,84	163.330,00	742.483,35
C	500-1000	8	512	18.096,96	124.272,82	1.138.958,27
D	250-500	16	384	15.609,00	66.990,82	1.321.597,11
E	100-250	32	256	13.093,44	31.262,38	1.419.386,32
F	50 - 100	80	128	8.527,32	13.398,16	1.754.038,71
G	< 50	209	64	5.774,28	13.398,16	4.007.040,77
TOTALE		**350**				**10.646.107,09**

Tabella D-6

La Tabella D-6 fornisce la stima del costo annuo totale (a regime) della RUPAR per quanto attiene ai canoni dei servizi di Trasporto e Interoperabilità ricavati dai correnti canoni della RUPA, che sono comprensivi della remunerazione dei Fornitori.

D.2.2.2 Altri costi

Ai costi relativi ai servizi di base di cui al paragrafo precedente, vanno aggiunti i costi relativi ad altri argomenti:

- Locazione degli armadi degli EPO
- Servizio Firma Digitale

La locazione degli armadi degli EPO è valutata in base ai parametri determinati dall'Autorità Garante delle Comunicazioni (AGCOM) nelle sue delibere n. 13/00/CIR e 14/00/CIR, per il servizio di colocazione di altri Operatori presso le Centrali di Telecom Italia.

A partire da tali dati, il canone annuo dell'alloggiamento di un telaio (LxPxH = 600x600x2200mm, area operativa circa 3 mq, accessibilità anteriore e posteriore, assorbimento elettrico fino a 2Kw) è stimato prudenzialmente in Euro. 7.500, fornendo quindi un totale di Euro. 30.000/anno per la locazione degli armadi di tutti e quattro gli EPO provinciali (quello di Bari è allocato presso il Centro Tecnico), tale stima è stata raddoppiata per tenere conto di eventuali future necessità di raddoppio dello spazio.

Il servizio di Firma Digitale prevede una dimensione di circa 10.000 certificati individuali (a regime) che rappresenteranno la stragrande maggioranza dei certificati utilizzati.

Questo quantitativo consente di poter dotare tutti i Responsabili delle Amministrazioni (Presidenti, Sindaci, Assessori, Dirigenti con potere di firma etc.) di una propria Firma Digitale, con cui poter firmare sia gli Atti dell'Amministrazione che potrebbero così essere resi pubblici direttamente in forma elettronica legalmente valida, sia le comunicazioni formali dirette ad altre Amministrazioni.

D.2.3 Determinazione dei criteri di copertura dei costi

Il POR 2001-2006 della Regione Puglia prevede, nell'Allegato 2 dei Complementi di Programmazione, un finanziamento pari al 50% del fabbisogno finanziario complessivo dell'Azione a) della Misura 6.3, previsto pari a Euro 45.000.000 per tutta la durata del Piano.

La restante quota del 50% del valore dell'Attività deve essere coperta dai Fornitori che in tutti e due i casi (Trasporto/Interoperabilità e Firma Digitale) effettuano quindi un investimento a fronte dei guadagni che potranno realizzare:

- mediante la vendita alle Amministrazioni di servizi aggiuntivi, non catalogati tra quelli basilari della RUPAR, quali per esempio servizi di comunicazione avanzati (Trasporto), servizi di ospitalità degli ambienti applicativi (Interoperabilità), certificati per server (PKI); si fa notare che questi servizi potranno essere erogati solo da Fornitori qualificati della RUPAR, che quindi godranno di una effettiva riserva di mercato
- mediante la vendita alle Amministrazioni di servizi aggiuntivi, non catalogati tra quelli basilari della RUPAR, quali per esempio servizi di consulenza e/o sviluppo applicativo, per i quali, pur non usufruendo di una riserva di mercato, la contiguità operativa e di servizio con le Amministrazioni è sicuramente un fattore trainante

- mediante continuazione del servizio dopo il periodo 2001-2006: si fa notare che alla fine del periodo 2001-2006 venendo meno il cofinanziamento del servizio da parte del POR, il costo dei servizi sarà interamente sostenuto al 100% dalle Amministrazioni.

La Regione Puglia quindi chiede ai Fornitori di Servizi un impegno di investimento a fronte del quale fornisce una riserva del mercato della PAL pugliese, il cui decollo è supportato mediante il finanziamento della restante quota del 50% dei costi, il che esclude oneri per gli Enti della PAL.

L'impegno di investimento dei Fornitori dovrà essere pari al 50% dei costi del servizio RUPAR che saranno determinati mediante apposita gara.

Questi costi saranno sostituiti ai costi stimati nel paragrafo precedente (Tabella D-6 e testo seguente), determinando così l'effettivo ammontare del costo totale del servizio e la quota parte del finanziamento a carico del POR.

D.2.4 Pianificazione del budget

La pianificazione del budget tiene conto del fatto che nel corso della parte rimanente dell'anno 2002 si provvederà ad una serie di attività propedeutiche all'attivazione, quali:

- preparazione dei bandi di qualificazione dei Fornitori
- attivazione del Centro Tecnico

di conseguenza si può prevedere che la totalità degli oneri ricadano nei quattro anni successivi.

In Figura D-1 è stato indicato l'obiettivo di crescita della RUPAR in termini di Enti collegati e su questa base è stato redatta la pianificazione del budget.

In dipendenza del numero di Enti collegati in RUPAR si è fatta una stima del numero dei Certificati di Firma Digitale necessari nei corrispondenti anni, ipotizzando una crescita non strettamente proporzionale con il numero degli Enti collegati, facondo dipendere il maggior numero degli ultimi anni dal compiuto avvio delle applicazioni.

D.3 Pianificazione temporale

La pianificazione di larga massima del budget della RUPAR è riportata nella seguente tabella:

Servizio/Anno	2003	2004	2005	2006	Totale (€)
Numero Enti	300	350	350	350	
Costi Trasporto	2.421.963	2.825.624	2.825.624	2.825.624	10.898.835
Costi Interoperabilità	6.703.271	7.820.483	7.820.483	7.820.483	30.164.721
Costi EPO	60.000	60.000	60.000	60.000	240.000
Numero Firme Digitali	5.000	6.000	8.000	10.000	
Costi Firme Digitali	175.000	210.000	280.000	350.000	1.015.000
TOTALE	**9.365.235**	**10.922.107**	**10.994.107**	**11.066.107**	**42.347.556**

Tabella D-7

Secondo questa pianificazione, il totale dei costi previsti nei quattro anni è comunque inferiore ai 45M€ previsti nel POR.
Nell'ipotesi che la ripartizione dei costi al 50% tra Fornitori ed Intervento Pubblico sia costante nei 4 anni, si ha un onere per l'intervento pubblico di circa 4,5 M€ entro il 31/12/2003, coerentemente con quanto già stanziato a cura della Regione Puglia.

E' comunque importante sottolineare che questa è una pianificazione di massima, realizzata a partire da valori unitari di costo di larga stima: la sua utilità risiede soprattutto nel fatto di aver permesso di consolidare il livello dell'intervento che è possibile realizzare con il sostegno finanziario del POR.

Il risultato è stato che è possibile pensare di servire fin dall'inizio la totalità delle PAL primarie (Regione, Province, Comuni) e una significativa parte delle altre Amministrazioni locali.

Il livello di servizio che si riesce a fornire è un livello basilare (Trasporto e Interoperabilità) più un nucleo iniziale di servizi di Firma Digitale indispensabili per il supporto sia di una più moderna modalità di espletamento della normale attività istituzionale che dell'avvio della Cooperazione Applicativa.

La ripartizione percentuale del valore complessivo dei servizi che verranno attivati sulla RUPAR è mostrata nel seguente grafico:

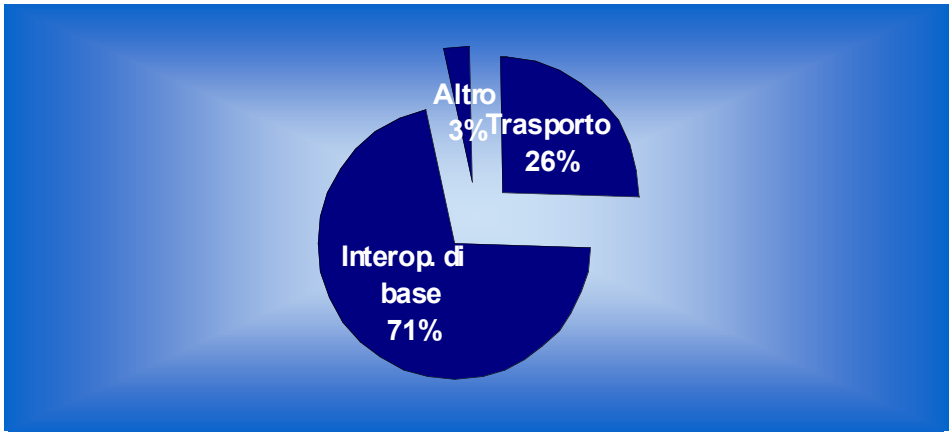


Figura D-2

E' il caso di notare che qualsiasi minore costo che si dovesse riscontrare nel corso dell'Esercizio, verrebbe destinato a potenziamenti nelle due possibili direttrici:

- ampliamento del numero di Enti serviti
- innalzamento del livello qualitativo/quantitativo dei servizi già forniti e/o pianificati

E' compito del Centro Tecnico monitorare l'evoluzione della RUPAR rispetto al budget pianificato, proponendo alla Regione le eventuali scelte possibili per una sua rimodulazione in corso d'opera.

D.3.1 Documenti ed atti esecutivi conseguenti al presente Piano

Successivamente all'approvazione del presente Piano da parte della Regione Puglia, verranno compiuti i seguenti passi:

- emanazione del Bando di qualificazione per i Servizi di Trasporto ed Interoperabilità
- emanazione del Bando di gara per il Servizio di Firma Digitale
- emanazione del Bando di appalto per la locazione degli armadi degli EPO

A seguito della pubblicazione dei Bandi si svolgeranno le gare.

L'esito delle prime due gare sarà la selezione di una certa quantità di Fornitori ritenuti idonei dal punto di vista tecnico e che avranno anche fatto le offerte economiche più vantaggiose rispetto al criterio previsto nel Bando.

Per il restante Bando l'esito della procedura d'appalto sarà l'individuazione di un Fornitore che provveda alla fornitura del servizio richiesto.

La pubblicazione dell'elenco dei Fornitori che risulteranno qualificati, permetterà alle Amministrazioni individuate nel presente Piano come beneficiarie finali dell'intervento, di scegliere il Fornitore da cui ottenere il servizio.

E' invece compito del Centro Tecnico operare congiuntamente con il vincitore dell'ultimo bando al fine di attivare:

- l'infrastruttura degli EPO
- l'infrastruttura del Centro Tecnico stesso

Queste infrastrutture sono propedeutiche all'attivazione delle infrastrutture degli altri Fornitori.

D.3.2 Individuazione dei soggetti interessati e dei relativi ruoli

I soggetti interessati sono i seguenti:

La Regione Puglia ha il ruolo di gestore del finanziamento POR e quindi di committente dell'intero complesso di attività; la Regione riveste anche il ruolo di utente della RUPAR in quanto è una della PAL che vi devono essere collegate.

Il Centro Tecnico, funzione ricoperta dalla società Tecnopolis CSATA s.c.r.l in virtù di quanto determinato nei Complementi di Programmazione del POR relativamente alla Attività b), Sottomisura A, Misura 6.3 del POR, ha il ruolo di controllore e di gestore dei servizi centrali della rete.

Le singole Amministrazioni individuate in Tabella D-1, e quelle che eventualmente dovessero aggiungersi successivamente in sede di rimodulazione dell'intervento, hanno il ruolo di beneficiarie finali dell'intervento

I FSR e i FSFD hanno sia il ruolo di fornitori di servizi che quello di investitori e cofinanziatori dell'iniziativa

D.3.3 Scadenze di attivazione

I Bandi verranno emanati subito dopo l'approvazione del presente Piano e verranno pubblicati con la scadenza prevista dalla Legge.

Successivamente allo svolgimento delle procedure di qualificazione e aggiudicazione è previsto un tempo di circa uno-due mesi durante il quale i Fornitori procederanno all'attivazione dell'infrastruttura dei propri servizi e simultaneamente il Centro Tecnico provvederà all'attivazione di quanto di propria competenza: EPO, Centro Servizi e collegamento a Internet; ed inoltre provvederà ad emanare i necessari regolamenti operativi sia di tipo tecnico che organizzativo ed economico.

In un arco temporale di circa 5 mesi, a partire dall'emanazione dei Bandi, si può quindi prevedere che la RUPAR sia pronta a collegare le prime Amministrazioni utenti.

D.3.4 Tempistica di esercizio

L'esercizio partirà dal momento in cui saranno espletate le fasi descritte nel paragrafo precedente, allo stato dell'arte nel corso di redazione dell'attuale versione del presente documento è presumibile che questo accada all'inizio del 2003.

A partire da quel momento i vari soggetti individuati nel paragrafo D.3.2 interagiranno per l'attivazione dei servizi.

La durata dei singoli contratti delle Amministrazioni con i Fornitori sarà sempre di un anno eventualmente rinnovabili in caso di mancata disdetta.
A scadenza normalmente annuale il Centro Tecnico attiverà una procedura di revisione dei costi per tenere conto della loro evoluzione nell'ambito del mercato ICT nazionale.

Ogni tre mesi il Centro Tecnico fornisce alla Regione Puglia un Rapporto sullo stato della Rete, contenente informazioni sia di tipo tecnico che organizzativo ed economico (andamento del volume di attività e del corrispondente onere a carico del POR).

D.4 Esercizio

D.4.1 Modalità di controllo da parte della Regione Puglia

Come accennato nel precedente paragrafo, la Regione Puglia eserciterà in controllo della RUPAR e delle attività ad essa connesse per tramite del Centro Tecnico, che rappresenta il braccio esecutivo della Regione in questo campo.

Il Centro Tecnico fornirà alla Regione un rapporto periodico in cui si saranno evidenziati i principali indicatori dell'andamento delle attività:

- numero ed elenco completo delle Amministrazioni collegate
- tipologia dei servizi da esse utilizzata
- statistiche di utilizzo dei principali servizi
- valutazione dell'impegno economico e sua compatibilità rispetto al budget

La Regione, in sede di analisi del Rapporto periodico, indicherà al Centro Tecnico le scelte che riterrà di effettuare a fronte di eventuali alternative che si dovessero porre circa l'evoluzione della RUPAR e dei servizi erogati per suo tramite.

D.4.2 Funzioni e responsabilità del Centro Tecnico

Il Centro Tecnico ha la responsabilità di gestire la RUPAR per conto della Regione e, in questa veste, svolge le seguenti funzioni:

- gestisce l'evoluzione della RUPAR dal punto di vista tecnico e funzionale, emanando quando necessario disposizioni tecniche per il corretto funzionamento dei servizi
- gestisce direttamente gli EPO e l'infrastruttura centrale dei servizi, ivi compresi il collegamento a RUPA
- controlla che i servizi vengano erogati dai Fornitori in conformità alle regole tecniche prescritte, a questo fine effettua anche audit nei loro confronti
- raccoglie dai Fornitori i dati di registrazione delle attività degli utenti, rendendoli disponibili a fini statistici e di pianificazione
- esplica attività di consulenza per la Regione e le altre Amministrazioni per supportare le loro scelte in ordine allo sviluppo di nuovi servizi basati su RUPAR
- valida i progetti dei nuovi sistemi di cooperazione applicativa che devono utilizzare la RUPAR, in ordine alla loro conformità agli standard tecnici e qualitativi previsti in RUPAR
- fornisce supporto ai Fornitori in ordine alla gestione di possibili malfunzionamenti della rete derivanti da problemi tecnici di altri Fornitori

L'insieme di queste funzioni, unitamente a quelle proprie della Struttura di Gestione per i servizi applicativi di cui al successivo paragrafo, sono svolte dal Centro Tecnico in virtù del mandato ad esso affidato nel quadro dell'Attività b), Sottomisura A, Misura 6.3 del POR.

D.4.3 Funzioni e responsabilità della Struttura di Gestione

La Struttura di Gestione dei servizi Applicativi è una funzione svolta dal Centro Tecnico della RUPAR al fine di fornire un primo substrato di funzionalità di supporto allo sviluppo di applicazioni cooperative sulla RUPAR.

Si è ritenuto utile fornire un supporto centralizzato che andasse oltre ai servizi di Trasporto e Interoperabilità di base, al fine di consentire lo sviluppo di soluzioni di cooperazione che fosse il più possibile sinergico e coerente, con conseguenti vantaggi dal punto di vista dell'efficienza e dell'economicità degli stessi.

Esempi di funzioni di supporto allo sviluppo applicativo sono i seguenti:

- infrastruttura centralizzata di PKI
- Portale dei servizi disponibili su RUPAR

- Servizio leggero di autenticazione basato su LDAP
- Servizio di Directory dei servizi applicativi (UDDI)
- Servizio di supporto alla segnalazione di eventi (Publish & Subscribe)

Questa funzione di supporto delle applicazioni è svolta dal Centro Tecnico in virtù del mandato ad esso affidato nel quadro dell'Attività b), Sottomisura A, Misura 6.3 del POR.

D.4.4 Funzioni e responsabilità dei fornitori di servizio

I Fornitori, una volta qualificati, possono interagire con le singole Amministrazioni per offrire i servizi base (Trasporto, Interoperabilità e Firma Digitale) per cui si sono qualificati.

Il livello di servizio base di cui ogni Amministrazione può usufruire sarà deciso, in quadro di compatibilità finanziaria complessiva, dalla pianificazione di cui alla Tabella D-7, rivista in funzione dei costi medi che emergeranno a valle dei Bandi di qualificazione.

L'Amministrazione potrà stipulare, se lo desidera, con il Fornitore un contratto per un livello di servizio superiore a quello pianificato, fermo restando che i maggiori oneri non saranno coperti dal finanziamento POR e quindi saranno dovuti dall'Amministrazione al Fornitore in dipendenza del prezzo pieno del servizio.

Il Fornitore potrà offrire alle Amministrazioni anche servizi aggiuntivi rispetto a quelli previsti di base nel presente documento, anche in questo caso gli oneri dei servizi aggiuntivi ricadono interamente sull'Amministrazione.

Il Fornitore è in ogni caso tenuto ad erogare i servizi in conformità agli standard tecnici prescritti dal presente documento e, più in dettaglio dal Bando di qualificazione, accettando eventuali prescrizioni e/o controlli del Centro Tecnico.

D.4.5 Flusso tecnico di monitoraggio del servizio

I servizi erogati su RUPAR saranno sottoposti ad un livello multiplo di monitoraggio:

- un primo livello, definito di "*sorveglianza*", è effettuato in tempo reale dal Fornitore del servizio, che è responsabile della sua corretta conduzione e deve intervenire per porre riparo ad ogni malfunzionamento al fine di garantire i livelli di servizio prescritti
- un secondo livello, definito di "*controllo*", è effettuato dal Centro Tecnico che analizza eventuali problemi rilevati dalla sua strumentazione, da audit periodici e/o da segnalazioni dell'utenza e prescrive ai Fornitori i rimedi da adottare
- un terzo livello, definito di "*pianificazione*", è effettuato dal Centro Tecnico che analizza i flussi di servizio della rete, sulla base dei dati che accumula mediante l'invio delle informazioni di traffico che i Fornitori sono tenuti ad effettuare, per valutare l'andamento dei servizi e progettare l'evoluzione dell'infrastruttura

Sono quindi individuabili due flussi principali dei monitoraggio:

- il primo che dal Centro Tecnico vede la propagazione di controlli periodici (per il servizio di Trasporto anche in tempo reale), verso le infrastrutture di servizio dei Fornitori
- il secondo che dagli apparati di servizio dei Fornitori vede un flusso di informazioni sul traffico degli utenti convergere verso il Centro Tecnico per l'archiviazione e successive elaborazioni.

Entrambi i flussi sono di capitale importanza per la corretta gestione della rete e quindi notevole importanza è attribuita dal Centro Tecnico alla disponibilità dei Fornitori di supportarli in modo effettivo.

D.5 Modalità di adesione da parte degli Enti

Le Amministrazioni che intendono avvalersi dei servizi della RUPAR hanno la possibilità di usufruire dei servizi descritti nel presente documento a costo zero fino al 31/12/2006, in quanto il relativo costo è coperto al 50% dal finanziamento POR al 50% dall'investimento dei Fornitori stessi.

A questo fine esse devono soltanto seguire l'iter procedurale descritto nel presente capitolo.

Va precisato che ogni informazione operativa relativa alla RUPAR ed al Centro Tecnico sarà resa disponibile sul World Wide Web alla url: **http://ct.rupar.puglia.it** subito dopo l'approvazione definitiva del presente documento e anticipatamente rispetto all'attivazione della RUPAR stessa.

Questo sito di informazioni, nel seguito riferito come "Sito Web del CT", avrà la funzione di facilitare l'avvio della RUPAR fornendo una fonte informativa e di interazione diretta con il CT.

D.5.1 Flusso formale di adesione alla RUPAR

L'Amministrazione la cui tipologia sia compresa tra quelle previste dalla Tabella D-1, potrà avvalersi di uno qualsiasi dei Fornitori che si saranno abilitati nel relativo Bando.
La lista dei Fornitori, dei servizi da essi offerti e dei relativi costi sarà disponibile sul Sito Web del CT.

L'Amministrazione potrà selezionare il Fornitore mediante una procedura di acquisizione di servizi infotelematici con procedura di Trattativa privata multipla ai sensi dell'art 7, comma 2b del T.U. dei Decreti Legislativi n. 157 del 17/3/1995 e n. 65 del 25/2/2000.
Infatti si è nel caso in cui i possibili fornitori di servizio sono predeterminati da vincoli tecnici (abilitazione ad operare su RUPAR), vi è inoltre nel periodo di validità del POR una convenienza economica ad avvalersi di un servizio che è coperto dal cofinanziamento regionale e del fornitore stesso.

L'Amministrazione dopo aver siglato i contratti con i Fornitori scelti, dovrà inviare via fax al CT copia dei loro Allegati di Sintesi, al fine di permettere al CT di inserire i relativi dati nella banca dati dell'utenza collegata. Il flusso finanziario relativo ai contratti è descritto nel successivo paragrafo D.5.5

D.5.2 Flusso tecnico di attivazione dei servizi

Il Servizio di Trasporto dovrà essere il primo ad essere attivato, successivamente dovrà essere attivato il Servizio di Interoperabilità di base; infine potrà essere attivata la disponibilità all'utilizzo del servizio di Firma digitale.

I tempi di attivazione di ogni servizio sono compresi nel SLA di cui al paragrafo seguente; l'Amministrazione deve rendere noti ad ogni suo Fornitore di Servizio i suoi eventuali altri Fornitori di servizi RUPAR.

Ogni Fornitore deve notificare il completamento delle attivazioni di propria competenza all'Amministrazione cliente ed al CT.

Le notifiche saranno effettuate via E-mail firmate digitalmente.

D.5.3 Accordo generale sui livelli di servizio (SLA, Service Level Agreement)

I livelli di servizio in termini di tempi di risposta del Fornitore alla richiesta del Cliente sono a fondamento dello SLA.
Per il Servizio di Trasporto essi non possono essere indipendenti da quelli previsti per la fornitura di linee affittate che sono stati fissati nella delibera 711/00/CONS della AGCOM.

Sulla base di quanto prescritto dalla delibera i tempi di consegna previsti devono essere conformi alla seguente tabella:

Velocità del servizio Trasporto	**Tempo massimo di consegna**
< 64 Kbit/s	Entro 35 giorni
64 Kbit/s - 2Mbit/s	Entro 50 giorni
2 Mbit/s	Entro 65 giorni
> 2 Mbit/s	Entro 125 giorni

I tempi sono calcolati a partire dalla data di firma del contratto di servizio fino alla data di effettiva consegna del servizio determinata dalle comunicazioni di cui al paragrafo precedente.

Per gli altri servizi il tempo massimo di consegna è di giorni 5.

Eventuali cause cogenti che possano impedire la consegna entro i tempi previsti dovranno sempre essere comunicate per iscritto sia all'Amministrazione che al CT, in ogni caso il Fornitore deve garantire il rispetto dei tempi indicati almeno nel 95% dei contratti in un anno, pena la revoca dell'abilitazione al servizio.

Ritardo	Penale
1-2 giorni solari	30% canone mensile
3-7 giorni solari	50% canone mensile
8-15 giorni solari	100% canone mensile
16-30 giorni solari	200% canone mensile
Oltre il 31-esimo giorno solare	Al 200% del canone mensile si aggiunge il 200% del canone giornaliero per ciascun giorno di ritardo

Per i giorni di ritardo nell'attivazione del servizio i relativi canoni fatturati alla Regione Puglia (per la quota finanziata) e/o all'Amministrazione (per la quota a suo carico) sono decurtati di quanto riportato nella seguente tabella:

Per quanto concerne le interruzioni di servizio, è stato definito per ogni servizio il livello di Uptime che deve essere rispettato.
Qualora il livello di *downtime* del servizio ecceda in un anno il massimo previsto, il canone annuale del servizio sarà decurtato in ogni sua componente del 25% di un canone mensile per ogni durata di *downtime* pari al 100% del massimo downtime previsto.

D.5.4 Standard contrattuali

Per l Servizio di Trasporto ed Interoperabilità verrà reso disponibile sul Sito Web del CT un contratto tipo, che potrà essere utilizzato come esempio per la stesura di un contratto tra Amministrazione e Fornitore.

Il contratto tipo conterrà sia la descrizione standard del servizio, sia le modalità di inserimento nel contratto di eventuali servizi aggiuntivi e la relativa modalità di gestione amministrativa dei costi, in conformità a quanto previsto nel successivo paragrafo.
Per il Servizio di Firma Digitale, ampiamente regolamentato dall'AIPA a livello nazionale, si ritiene superflua la predisposizione di uno specifico modulo contrattuale.

D.5.5 Flusso finanziario relativo alla copertura dei costi

La fatturazione dei servizi erogati in ambito RUPAR sarà effettuata dal Fornitore interamente nei confronti dell'Amministrazione utente.
La fatturazione dovrà evidenziare:

- La quota di costo relativa ai servizi coincidenti con quanto previsto dalla pianificazione della RUPAR per la specifica Amministrazione, destinata ad essere coperta dal finanziamento pubblico (50% del Costo di Riferimento coperto dal POR).
- La quota di costo per i servizi eccedenti quanto previsto per l'Amministrazione dalla pianificazione della RUPAR: l'eccedenza concerne sia un livello più elevato di un servizio previsto, sia un servizio aggiuntivo (opzionale)

L'Amministrazione potrà chiedere alla Regione Puglia la copertura finanziaria della prima quota di costo, utilizzando la rendicontazione prevista per la Misura 6.3 del POR.

Tecnopolis CSATA

Regione Puglia

Centro Tecnico della R.U.P.A.R. Puglia

Progetto del Centro di Erogazione Servizi Tecnologici del Centro Tecnico

(prodotto nell'ambito della Convenzione approvata dalla Giunta Regionale con deliberazione n. 1162 del 10/8/2001)

Allegato B

Versione 1.6 del 31 luglio 2002

INDICE

Capitoli

Figure

Tabelle

1 Introduzione

Il progetto concerne la progettazione funzionale, tecnologica ed esecutiva del Centro di Erogazione Servizi Tecnologici (**CEST**) del Centro Tecnico della rete RUPAR Puglia.

Le parti funzionale e tecnologica del progetto hanno valenza generale, mentre la parte esecutiva, dovendosi relazionare alle infrastrutture fisiche (ambienti, potenza elettrica, cablaggio dati etc.) in cui il CEST si troverà ad operare al suo avvio, concernerà la situazione logistica e tecnologica del Parco Scientifico Tecnopolis a Valenzano.

L'infrastruttura denominata CEST è destinata a supportare il Centro Tecnico della RUPAR Puglia in tutte le sue attività di controllo, supervisione, coordinamento e relazionamento di sua competenza nell'ambito della gestione della rete.

Il presente progetto non descrive le suddette attività e funzioni del Centro Tecnico ma piuttosto provvede a progettare le funzionalità tecniche che il CEST deve supportare, a precisarne le componenti tecnologiche, il loro dimensionamento, la loro interconnessione fisica ed infine il loro costo previsto.

2 Obiettivi e Requisiti Funzionali

La missione affidata al CEST è di supportare tutte le funzioni tecnologiche della RUPAR mediante la gestione delle seguenti Applicazioni di servizio centrali:

- Portale del Centro Tecnico e dei Servizi RUPAR
- Sistema di Gestione Eventi e Directory dei Servizi per la Cooperazione Applicativa
- Sistema centrale di gestione e fruizione delle statistiche della rete
- Sistema di controllo e monitoraggio della rete
- Servizi tecnici centrali: Gestione dei nomi e dei domini (DNS), Servizio di Directory del CT (LDAP), Network Time Protocol Infrastructure, Posta Elettronica del CT

Inoltre il CEST deve soddisfare un serie di requisiti funzionali e tecnologici, dei quali si riporta la lista sintetica:

1. essere interconnesso alla RUPAR sul nodo di Bari
2. essere accessibile da Internet per tutti i suoi servizi destinati alla fruizione dei cittadini
3. erogare i servizi con un elevato *uptime*, superiore a quello richiesto ai Fornitori per i servizi di Trasporto ed Interoperabilità di base della RUPAR
4. garantire prestazioni di servizio che non rappresentino in alcun momento un collo di bottiglia rispetto al funzionamento complessivo della RUPAR
5. garantire sempre al massimo livello la sicurezza delle informazioni e dei servizi gestiti

Nei paragrafi seguenti sono esposte le scelte architetturali e tecnologiche che meglio consentono di soddisfare gli obiettivi ed i requisiti di cui sopra.

3 Progetto Funzionale

I due requisiti di erogare i servizi con un elevato *uptime* e prestazioni di alto livello portano inevitabilmente alla scelta di disegnare il CEST basandolo su una completa ridondanza di tutte le componenti tecnologiche.
Di conseguenza ogni componente funzionale deve essere, a livello tecnologico, almeno duplicata e devono essere realizzate tutte le funzionalità tecniche che consentono, in caso di guasto di una componente, di continuare ad erogare il servizio in modo trasparente per l'utente utilizzando la seconda componente.

Questo criterio generale di duplicazione di tutte le componenti, porta anche a soddisfare il requisito prestazionale tutte le volte in cui si riesce a far lavorare simultaneamente le due componenti, ripartendo su entrambe il carico complessivo di lavoro, che poi sarà sopportato dalla componente superstite in caso di guasto dell'altra: questa configurazione è generalmente definita a "**Condivisione di carico**" o "***Load balancing***" o "***Load sharing***".
Questo tipo di configurazione sarà adottato in modo esteso per la maggior parte delle componenti; qualora non dovesse essere praticabile per vari motivi, si adotterà una configurazione in cui la seconda componente, originariamente scarica di lavoro ed in attesa di entrare in servizio ("*Stand-by*"), subentra automaticamente all'arrestarsi della prima, senza che le applicazioni risentano di alcuna interruzione: questa configurazione è generalmente definita di "**Alta Disponibilità**" (**HA** o ***High Availability***) oppure di "***Stateful failover***".

Esistono alcuni servizi, come il Name server o la Posta Elettronica, per i quali è lo stesso standard che disciplina le modalità di ridondanza (concetto di server primario e secondario): questi casi sono assimilabili al caso di Alta Disponibilità.

La specifica modalità di configurazione di ogni componente funzionale sarà precisata nel paragrafo di progetto tecnologico in quanto dipende anche dalle specifiche tecnologie hardware e software scelte per l'implementazione dei servizi.

Le configurazioni in modalità di ripartizione di carico (*Load Balancing*) possono essere realizzate con molteplicità maggiore di due, al fine di migliorare ulteriormente le prestazioni. Nelle figure seguenti si potrà vedere che la molteplicità indicata è sempre pari a due; questo per la essenziale ragione che questa configurazione, che è la minimale per soddisfare entrambi i requisiti di uptime e *performance*, è anche ritenuta sufficiente a livello prestazionale per la fase di avvio del Centro Tecnico e probabilmente non necessiterà di revisione nei primi due-tre anni di esercizio.

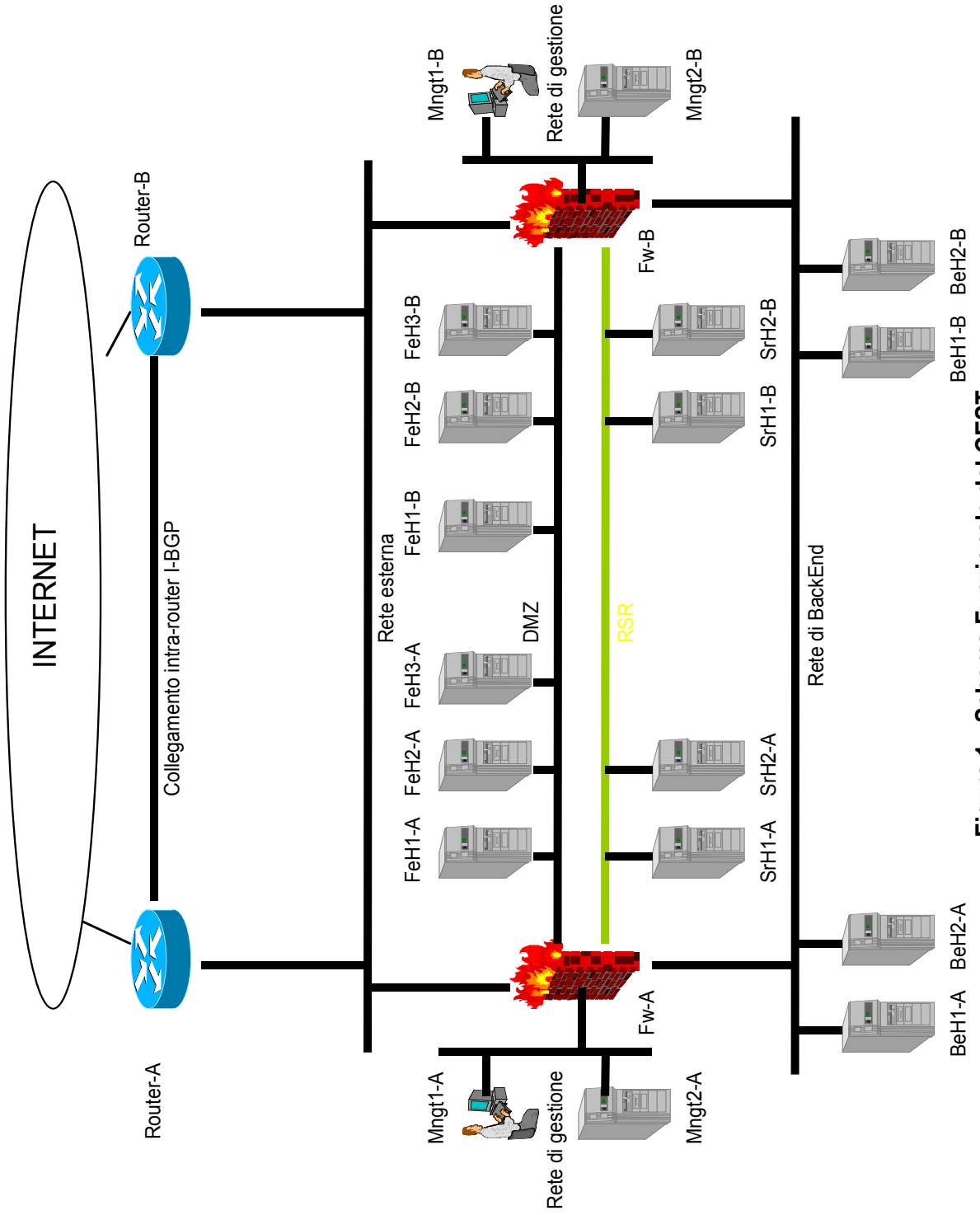


Figura 1 - Schema Funzionale del CEST

Nello schema in figura sono indicati gli elaboratori destinati all'erogazione dei servizi; ognuno di essi è contraddistinto con una sigla il cui prefisso ne indica l'allocazione su una specifica rete tra le seguenti:

- rete DMZ o rete di Front End: prefisso ***Fe***…
- rete RSR o rete dei Servizi Rupar: prefisso ***Sr***…
- rete di Back End: prefisso ***Be***…
- rete di Management: prefisso ***Mngt***…

Nella stessa sigla ogni elaboratore è identificato, oltre all'indicatore numerico, anche da un suffisso letterale che può essere **A** o **B,** che indica la ridondanza, per cui due elaboratori con identica sigla ma con suffisso diverso sono due elaboratori che svolgono al stessa identica funzione in configurazione di *Load Sharing* o di *Failover*.

La seguente tabella riporta la distribuzione dei servizi sui diversi elaboratori:

Elaboratore	**Funzione**	**Servizi**
Router	Connessione ad Internet	Trasporto
Fw	Firewall	Sicurezza
FeH1	HTTP Listener (Web cache)	Portale per il Cittadino e Fornitori
FeH2	LDAP Server	Directory organizzazione e PKI
FeH3	Name Server, Email Server	Gestione nomi, Posta elettronica (con antivirus)
SrH1	http Listener (Web cache)	Portale per la PAL, Gestore Eventi
SrH2	LDAP Server, Time Server	Directory dei Servizi e Sincronizzazione orario
BeH1	Application Server	Portale, Gestione Eventi, Directory dei servizi
BeH2	Database Server	Dati di tutti i servizi
Mngt1	SNMP manager	Monitoraggio e controllo
Mngt2	Proxy server ed Email Server	Navigazione (con antivirus) e Posta Elettronica

Tabella 1 - Allocazione dei principali servizi sugli elaboratori del CEST

4 Progetto tecnologico

Il progetto tecnologico specifica sia la parte rete di comunicazione dati in termini di maggior dettaglio, sia le singole piattaforme di elaborazione in termini di dimensionamento hardware, Sistema Operativo e principali *middleware* da utilizzare.

Le scelte che sottendono al progetto tecnologico sono le seguenti:

- Apparati di Front End (reti DMZ e RSR) di tipo “leggero” (piattaforme Intel a 32 bit con S.O. Linux) con software in gran parte di tipo *Open Source*
- Apparati di networking e di sicurezza di un unico fornitore leader di mercato
- Apparati di Back-End basati su:
    - piattaforme hardware di tipo Risc a 64 bit
    - sistema operativo UNIX a 64 bit
    - middleware di tipo Application Server e Database Server

La configurazione effettiva della ridondanza prevede la differenziazione tra server primario e secondario (come specificata dai relativi standard) per i seguenti servizi:

- Name Server
- Email Server
- Network Time Server
- LDAP Server

Mentre si basa su specifici meccanismi tecnologici, quasi sempre realizzati dai costruttori, per i seguenti servizi:

- Routing
- Firewall
- HTTP Listener o Web Cache (include Portale)
- Application Server (include Portale)
- Database Server

Il seguente schema illustra in maggior dettaglio il funzionamento di questi meccanismi:

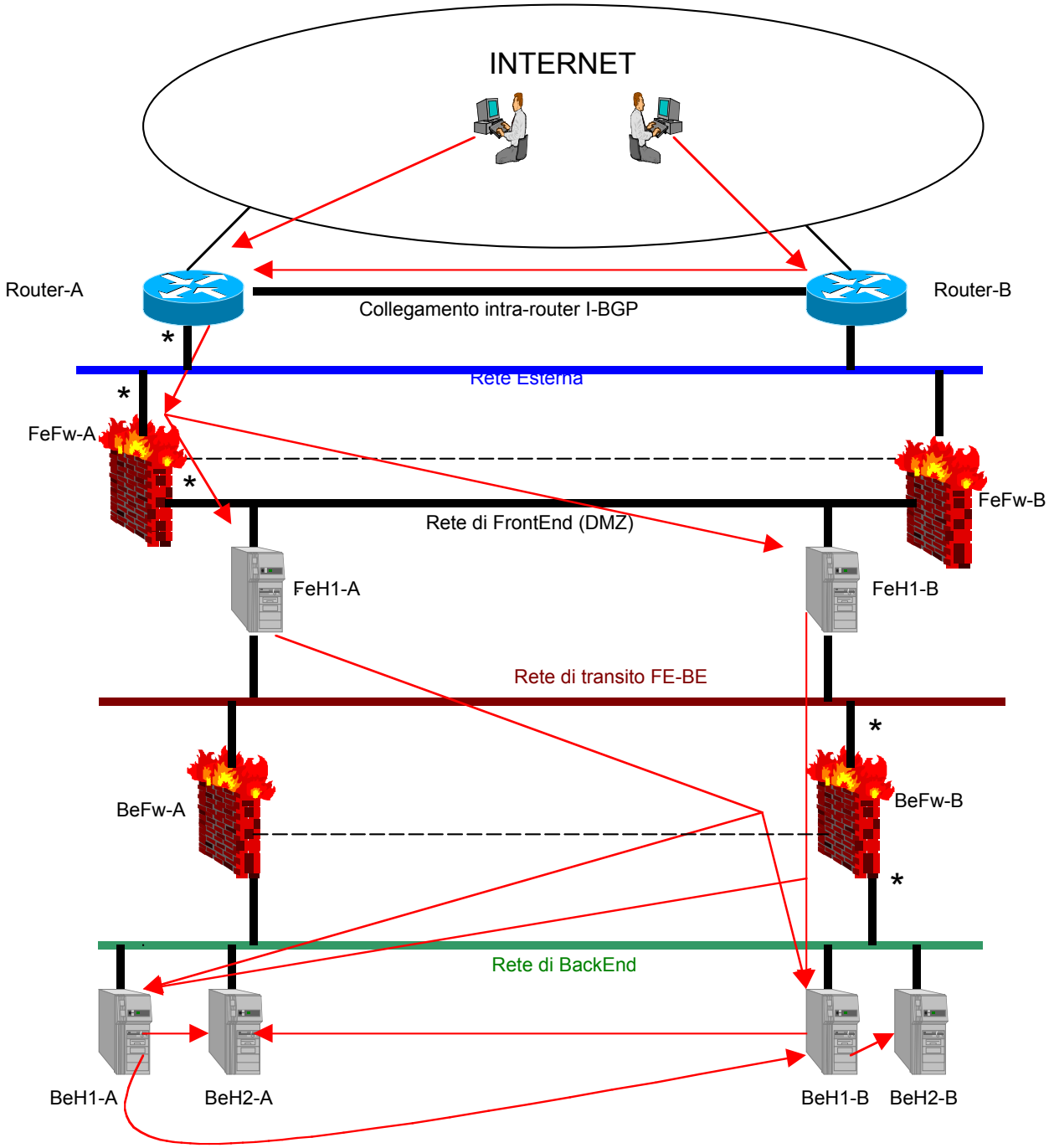


Figura 2 - Funzionamento della ridondanza dei servizi

La figura illustra il funzionamento nel caso della DMZ; ovviamente, nel caso della RSR (non riportata per semplificare lo schema), il meccanismo rimane lo stesso.
Si ricorda che la rete RSR è la "DMZ esclusivamente riservata alla RUPAR Puglia".

A differenza dello schema generale rappresentato in Figura 1, la piattaforma Firewall inserita nella Figura 2 risulta duplicata in quanto questa configurazione è quella che garantisce al massimo la sicurezza e permette a sua volta di ripartire il carico del traffico verso l'esterno e del traffico tra i sistemi di Front End e quelli di Back End
Nella figura precedente, le frecce indicano le direttrici di traffico attive in un dato momento; si noti che due utenti possono accedere ai servizi del CEST utilizzando entrambi i canali Internet di cui lo stesso CEST dispone.

Questa è la prima duplicazione, concernente il canale di accesso e serve a garantire la **continuità del servizio** del CT RUPAR anche in presenza di interruzioni del servizio di collegamento ad Internet da parte di uno dei due fornitori. Questa configurazione, definita nella letteratura tecnica come "*dual homing*", funziona mediante l'utilizzo del protocollo BGP da parte dei due router (A e B) che sono contemporaneamente attivi e si scambiano traffico attraverso il collegamento intra-router I-BGP.

La configurazione, che è una tipica configurazione a condivisione di carico rispetto ai collegamenti a Internet (che vengono quindi simultaneamente sfruttati) e rispetto ai due router, è in grado di resistere, continuando a garantire il servizio, nel caso di qualsiasi singolo guasto (linea o router).

Ovviamente questa configurazione è tanto più significativa, per quanto concerne i guasti di linea, tanto più i due percorsi fisici dei collegamenti sono differenziati, in modo che non possano verificarsi interruzioni di entrambi.

I due router che sono contemporaneamente attivi verso l'esterno (rete Internet) adottano, invece, verso l'interno (verso la "Rete Esterna") una tipica configurazione in alta disponibilità, per cui solo un collegamento (quello contrassegnato con l'asterisco) è attivo; l'altro router (Router-B) rimane in *stand-by* e subentrerebbe in caso di guasto del primo router (Router-A) ereditando tutte le caratteristiche necessarie a rendere trasparente l'operazione alle altre macchine in rete.
Nella figura tutte le interfacce di rete contrassegnate con un asterisco corrispondono ad apparecchiature che operano in alta disponibilità, per cui solo quella contrassegnata realmente smista il traffico, mentre l'altra corrispondente, accesa, entra in funzione se rileva un arresto della prima.
A funzionare in questo modo sono:

- i due router, limitatamente all'interfaccia sulla rete esterna
- le due coppie di Firewall (FeFw-A, FeFw-B e BeFw-A e BeFw-B) che hanno il compito di garantire la sicurezza dell'accesso ai servizi, in figura sono mostrati attivi il FeFw-A ed il BeFw-B, in pratica per migliorare le prestazioni e la sicurezza, la funzione di Firewall indicata in Figura 1 - Schema Funzionale del CEST viene sdoppiata su due coppie di apparati Firewall distinti (FeFw e BeFw).

La linea tratteggiata in figura tra i due Firewall indica l'esistenza di collegamenti dedicati di controllo per la gestione del processo di *polling*/*heartbeat*.

A valle del Firewall di Front End attivo il traffico viene bilanciato tra i due elaboratori di Front End (FeH1 ed FeH2), che ospitano le funzioni di **HTTP listener** e **Web cache** e lavorano in condivisione di carico. L'intero sistema è in grado di procedere con un solo elaboratore di Front End in caso di guasto dell'altro, senza che l'utenza si accorga di nulla.

Il bilanciamento del traffico tra i due elaboratori è effettuato da un apparato che non è mostrato in figura ed è lo Switch che realizza fisicamente tutte le reti locali indicate nella figura con un tratto di linea più spesso.

Si tratta di uno switch ad alte prestazioni con capacità di realizzare delle reti locali virtuali (V-LAN) e di gestire il traffico in base alle informazioni presenti anche a livello applicativo (***Content Switching***).

Tutto il traffico entrante è quindi indirizzato ai due elaboratori di Front End che lo elaborano utilizzando i servizi degli Application Server (BeH1 e BeH2), che si trovano sulla rete di Back End ed operano anch'essi in condivisione di carico grazie al bilanciamento che in questo caso è effettuato direttamente dagli elaboratori di Front End.

Il traffico tra Front End e Back End è inoltrato attraverso al rete di transito FE-BE, su cui opera la coppia di Firewall di Back-End, anche in questo caso in configurazione di Alta Disponibilità.

Questa configurazione, oltre ad essere a prova di singolo guasto come già detto, è considerata la più sicura in quanto i server applicativi ed il server di database si trovano su una rete (rete di Back End) che non è direttamente accessibile da Internet. Si noti che i flussi traffico tra Front End e Back End, mostrati per chiarezza come frecce dirette in figura, in realtà passano sempre dal Firewall attivo di Back End che in questo caso è il BeFw-B.

Finora abbiamo visto che la funzionalità di condivisione di carico è stata supportata a livello Front End mediante la capacità dello Switch di rete di ripartire il traffico tra i due elaboratori gemelli di Front End, mentre per il traffico FE-BE sono gli stessi elaboratori di Front End a indirizzare il bilanciamento in funzione di logiche strettamente applicative.

L'ultimo flusso di traffico è quello mediante il quale i primi Back End Host (BeH1-A e BeH1-B), sui quali è attivo l'Application Server, accedono ai dati memorizzati sugli altri due Back End Host (BeH2-A e BeH2-B) che ospitano il Database. Questi ultimi sono configurati come un'unica macchina virtuale (***Cluster***) la cui capacità di ripartire il carico tra i due elaboratori è gestita dal Sistema Operativo e dal software stesso del Database.

Il seguente schema illustra quindi la configurazione effettiva del CEST.
Si noti la presenza, nella rete di Back End, dei dispositivi di memorizzazione esterni (*Storage* Esterno) per le piattaforme di elaborazione Risc UNIX identificate dalle sigle BeST-A e BeST-B.

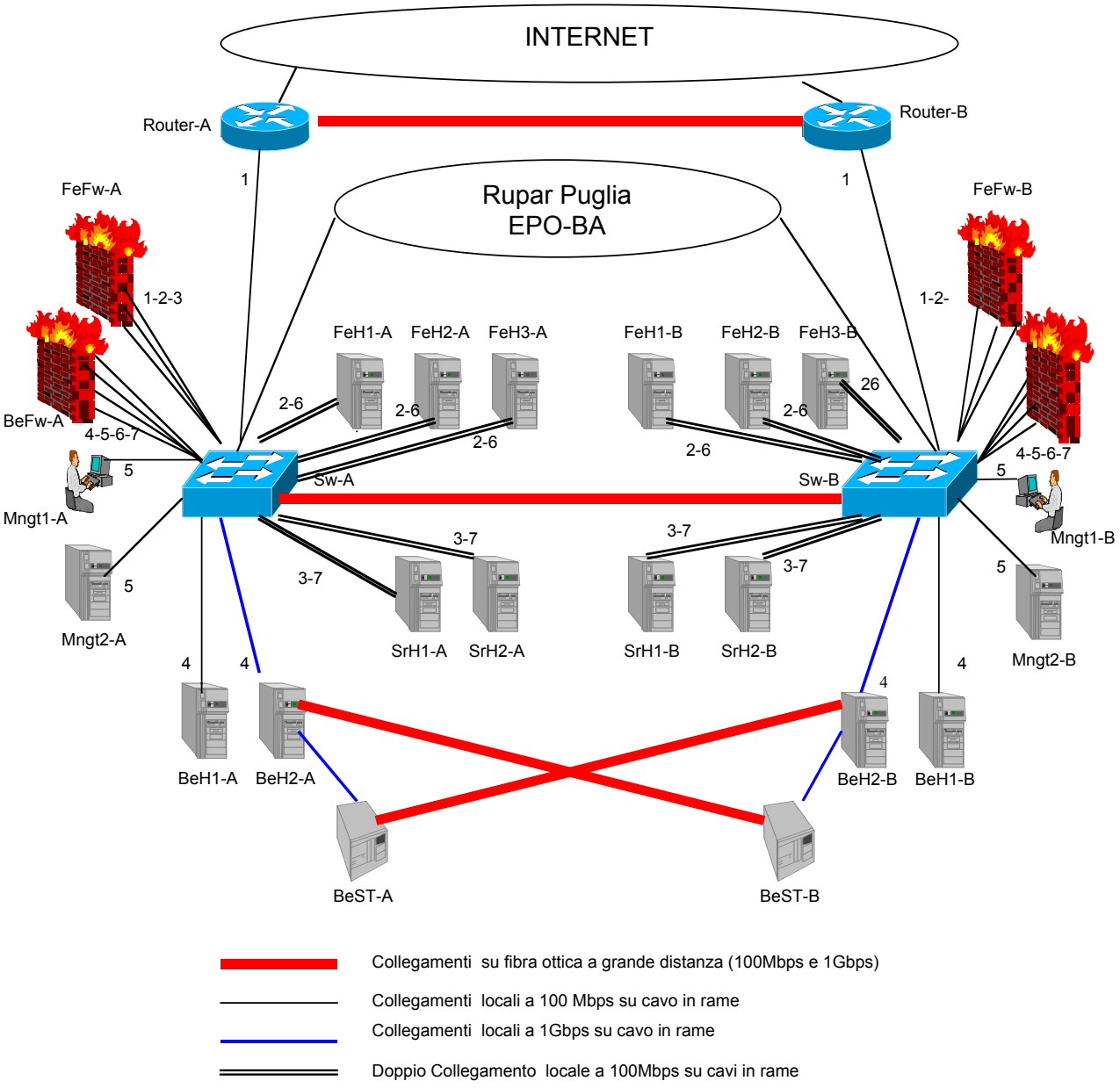


Figura 3 - Schema Tecnologico del CEST

Nella figura si può notare che tutte le reti indicate nello schema funzionale sono realizzate per mezzo dell'apparato Switch posto al centro di ognuna delle due parti del CEST. Questo tipo di apparati è in grado di realizzare reti virtuali e in prossimità di ogni collegamento dei diversi sistemi è appunto indicata la ***Virtual Lan*** (**VLAN**) cui si deve collegare il sistema; quando uno stesso sistema si collega, mediante più interfacce di rete, a diverse VLAN, queste sono indicate con i numeri di VLAN separati dal carattere '-'. L'apparato è in grado di effettuare anche il bilanciamento del traffico tra più elaboratori in base a diverse regole di tipo applicativo.

L'elenco delle V-LAN definite è il seguente:

- VLAN-1: rete esterna
- VLAN-2: rete DMZ o rete di Front End: prefisso ***Fe***…
- VLAN-3: rete RSR o rete dei Servizi Rupar: prefisso ***Sr***…
- VLAN-4: rete di Back End: prefisso ***Be***…
- VLAN-5: rete di Management: prefisso ***Mngt***…
- VLAN-6: DMZ vs. Back End transit network
- VLAN-7: RSR vs. Back End transit network

La figura mostra anche l'interconnessione press il CEST dell'EPO-LP di Bari e, per suo tramite, di tutta la RUPAR Puglia.

Questa interconnessione è meglio illustrata nel successivo paragrafo.

5 Gli EPO-LP della RUPAR

Il Centro Tecnico ha inoltre il compito di approntare e gestire i nodi della RUPAR Puglia, definiti EPO-LP (Exchange Point Operator, Locale Privato).

Come già definito nel documento di Progetto Strategico della RUPAR, un EPO-LP è costituito da un armadio contenente uno switch ad alte prestazioni (Gigabit/Fast Ethernet) ed un router di interconnessione per ogni Fornitore di Servizi RUPAR (FSR) attivo.

Il seguente schema illustra la funzionalità di un EPO-LP.

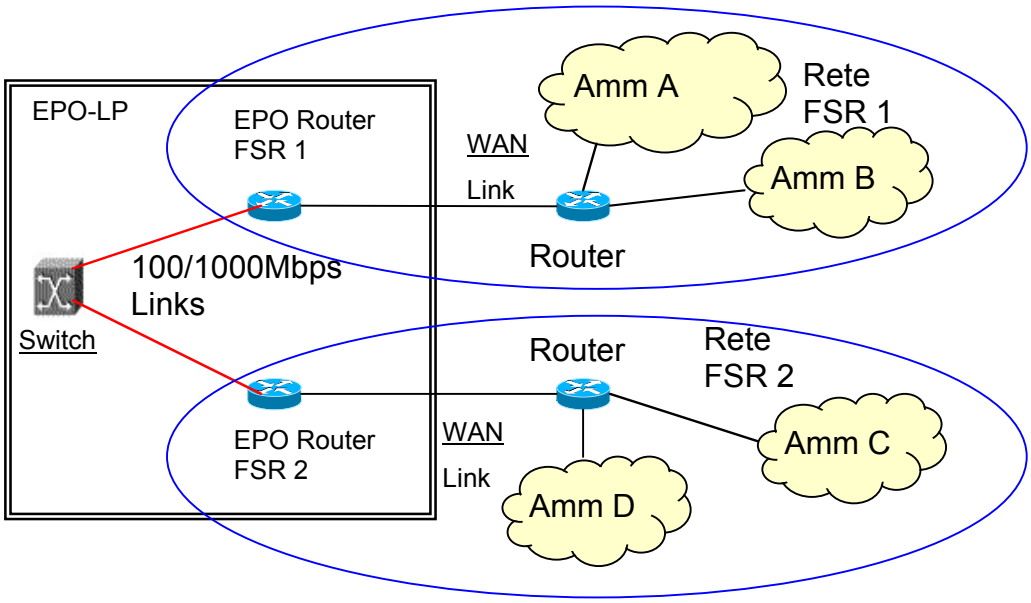


Figura 4 - Schema di un EPO-LP della RUPAR

Compito del Centro Tecnico è di rendere disponibili e successivamente gestire l'armadio e lo switch di interconnessione, mentre ogni singolo Fornitore dovrà attivare e gestire i propri router.

L'EPO-LP di Bari sarà allocato presso il Centro Tecnico e strettamente interconnesso alla sua infrastruttura tecnologica. La sua caratteristica saliente sarà quella di essere completamente ridondato così come tutto il CEST, in modo da garantire sempre la propria attività ed anche la funzione di back-up automatico degli EPO-LP provinciali nel caso di un loro guasto.

Lo Switch di livello 2 che realizza fisicamente la funzione di interconnessione dell'EPO-LP di Bari sarà costituito dalla stessa coppia di Switch principali del CEST, sui quali sarà attivata un'altra VLAN per questo servizio.

Inoltre l'EPO-LP di Bari sarà dotato di una coppia di router, in questo caso distinti da quelli già presentati nei precedenti schemi del CEST, che avranno la principale funzione di consentire l'accesso ai servizi del CEST da parte di tutta la RUPAR.
Questi router, denominati nella successiva figura EPO-Router A e B, dialogheranno mediante il protocollo BGP con i router dei Fornitori allocati nell'EPO-LP di Bari.
La protezione dell'EPO-LP di Bari sarà garantita dalla coppia di Firewall posti a protezione esterna del CEST.

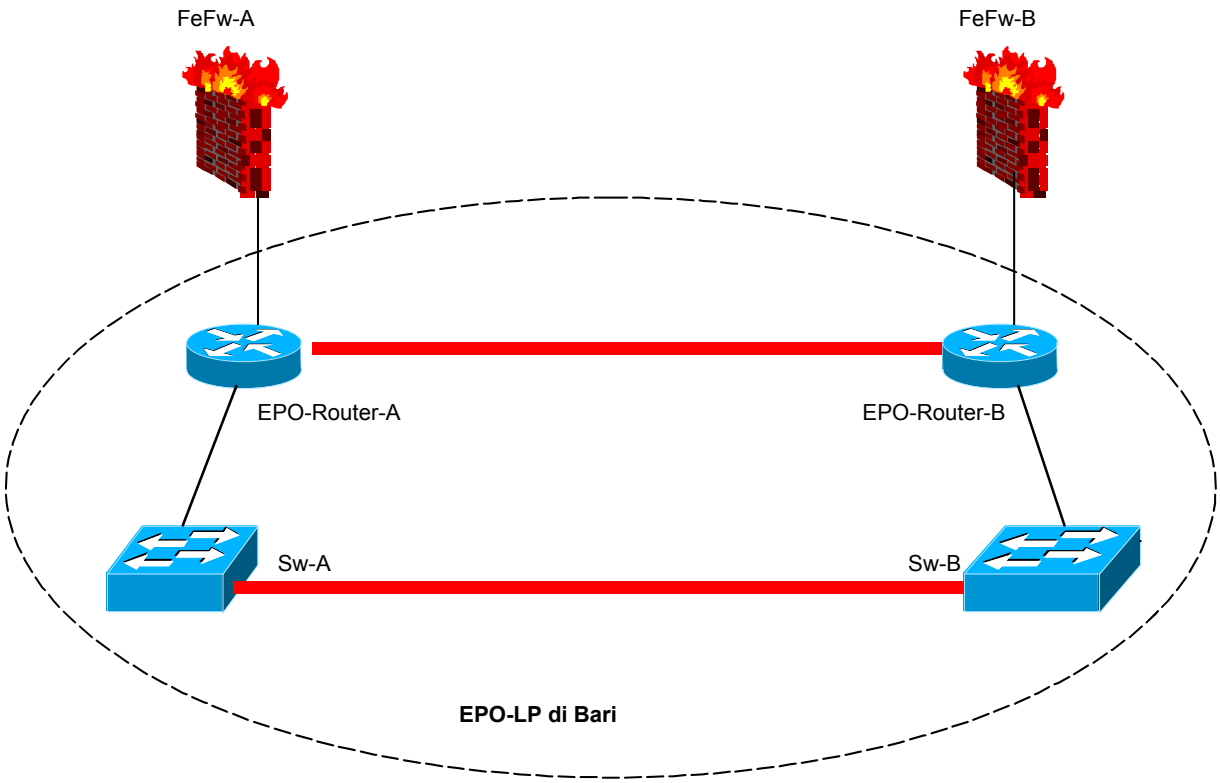


Figura 5 - Schema dell'EPO-LP di Bari

6 Il Sistema CIFRA

Il Centro Tecnico, in virtù di quanto previsto nella Convenzione che ne regola l'attività, ha in carico la gestione tecnica e l'evoluzione tecnologica del Sistema Informativo CIFRA che provvede alla gestione informatizzata delle Delibere della Giunta Regionale ed è gestito dal punto di vista funzionale dalla Segreteria della Giunta.

Il servizio CIFRA, già operativo da diversi anni, deve essere potenziato in termini di Hardware e Software di base, intendendo per quest'ultimo il middleware di gestione del Workflow su cui sistema CIFRA si basa.

Il potenziamento concerne la sostituzione dell'attuale server principale di erogazione, allocato nel CED della Presidenza della Giunta Regionale, con un server configurato in cluster e quindi interamente ridondato ed in grado di operare in condivisione di carico tra le sue due unità, garantendo così sia le prestazioni, per quanto concerne i tempi di risposta, che la continuità di servizio a fronte di qualsiasi singolo guasto.

Oltre al server principale, che dovrà sostenere l'aumento del carico derivante dall'ampliamento dell'utenza interna della Regione Puglia che farà uso del sistema CIFRA e dei relativi servizi di gestione informatizzata dell'iter delle delibere, si prevede di rinnovare sia il server che consente l'accesso via Internet alle informazioni rese disponibili dallo stesso servizio (CIFRAWEB), sia il server di aggiornamento/backup che ha funzioni di supporto tecnico all'ambiente di esercizio.

Lo schema finale risultante del servizio CIFRA, inserito nel contesto RUPAR, è riportato nella seguente figura, tratta dallo schema generico, contenuto nel Piano Strategico della RUPAR, della Porta di Rete (PdR), di cui costituisce una specifica specializzazione.

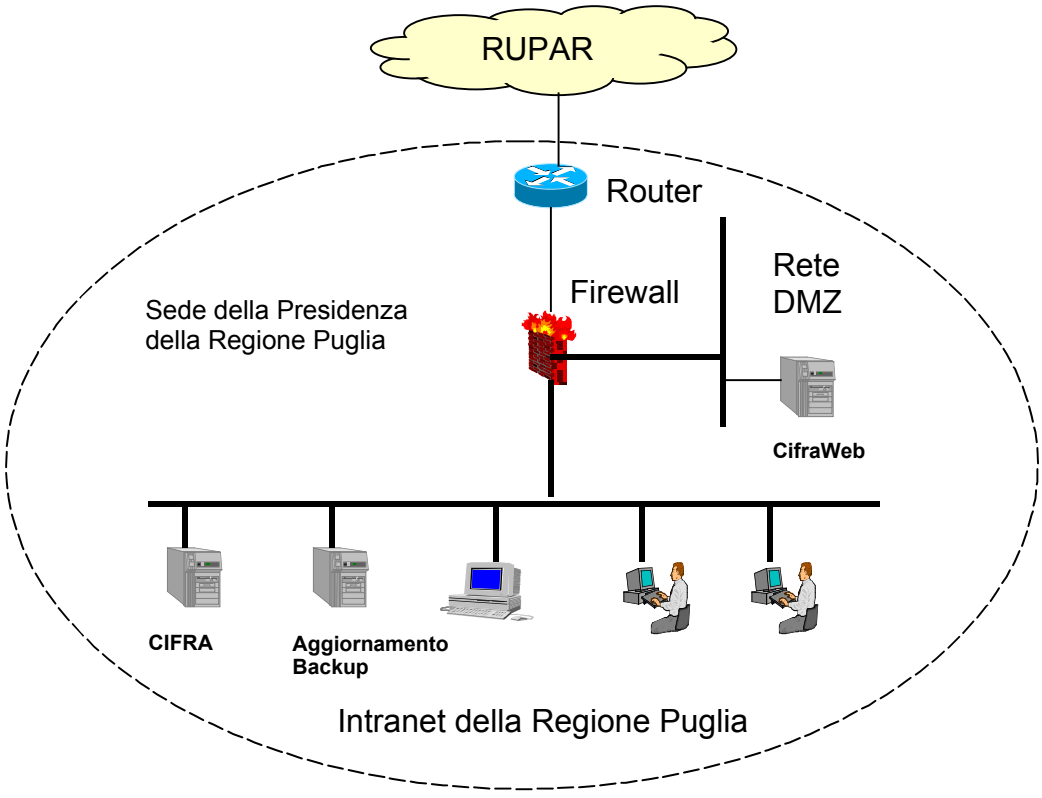


Figura 6 – Sistema CIFRA e sua collocazione in rete

7 L’acquisizione della strumentazione

Per l’approvvigionamento della strumentazione si prevede di ripartire l’investimento in più lotti indipendenti e omogenei dal punto di vista tecnologico e funzionale, al fine di ottenere, mediante la specializzazione dei fornitori, la massima qualità di ogni singola parte della fornitura e contemporaneamente anche le migliori condizioni economiche.

In particolare, si intende procedere, seguendo le procedure già stabilite nel quadro della Convenzione con la Regione Puglia, con l’espletamento di 5 lotti di fornitura così come da tabella seguente.

Lotto	Descrizione Intervento
Lotto 1: Sistemi di *Front-End*, di Management ed accessori di gestione del CEST	• n.8 server monoprocessore basati su CPU Intel • n.8 server biprocessore basati su CPU Intel • n.16 PC desktop + n.2 DAT 20/40 GB esterni • n.2 armadi tecnici per ospitalità apparati di Front-End • n.16 PC portatili P III Enhanced Speed Step Technology con Smart Card Reader • n.1 Stampante laser + n.1 stampante inkjet • n.16 Cellulari GSM con supporto HSCSD e modem integrato
Lotto 2: Rete dati e sicurezza del CEST e apparati EPO	• Apparati di rete interna e geografica (Switch, Router e Firewall in configurazione ridondata) • n.2 armadi tecnici per ospitalità apparati di rete e sicurezza • Apparati per attrezzare gli EPO-LP • n.6 armadi tecnici per ospitalità apparati in EPO-LP
Lotto 3: Sistemi di *Back-End* del CEST	• n. 1 Cluster HA 2xbiprocessore Risc per Database Server • n. 2 server Risc biprocessore per Application Server • n. 2 sistemi di Storage con 576 Gbytes totali utili ed infrastruttura FiberChannel per accesso flessibile ai dati • sottosistema di backup centralizzato • n.2 armadi tecnici per ospitalità apparati di Back-End • software Database ed Application Server inclusivo di ambiente per lo sviluppo e la manutenzione di portali Web • software applicativo per la funzionalità di **Gestione Eventi,** che è alla base della cooperazione applicativa. L'applicazione rispetta il modello "*Publish and Subscribe*" e consente l'inoltro automatico e sicuro di messaggi (eventi) dall'ente pubblicatore (*publisher*) agli enti sottoscrittori (*subscriber*)
Lotto 4: Lavori di adeguamento sicurezza CEST	• lavori di miglioramento della sicurezza fisica (separatezza) degli ambienti destinati ad ospitare gli apparati del CEST • fornitura e posa in opera di strumentazione specializzata per la regolamentazione degli accessi nei locali destinati ad ospitare gli apparati del CEST
Lotto 5: Sistemi Hw/Sw per il servizio CIFRA	• n. 1 Cluster HA 2xmonoprocessore Intel per Database ed Application server principale • n. 1 server Intel monoprocessore per Web Application Server e • n. 1 server Intel monoprocessore per funzioni di aggiornamento e supporto • versioni aggiornate middleware di workflow comprensivo di database e application services • n.1 armadio tecnici per ospitalità apparati

Tabella 2 - I Lotti e gli apparati da acquisire

Per tutti le forniture Hw/sw dei diversi lotti si intende richiedere l'installazione, l'avviamento e la manutenzione per almeno 2 anni on-site di tutta la strumentazione fornita.

Nei paragrafi seguenti, invece, si descrive la dislocazione degli apparati, il progetto impiantistico ed il costo stimato dell'intero progetto.

8 La dislocazione degli apparati del CEST

Tutti gli apparati saranno in configurazione da "*rack*" e, di conseguenza, saranno installati nei relativi armadi.

Più precisamente il nucleo principale CEST sarà costituito da due coppie identiche (A e B) di un gruppo di tre Armadi (dimensione standard 19" in larghezza e 42 unità in altezza) che conterranno tutte le apparecchiature.

I tre Armadi di ogni gruppo sono schematizzati nella seguente figura:

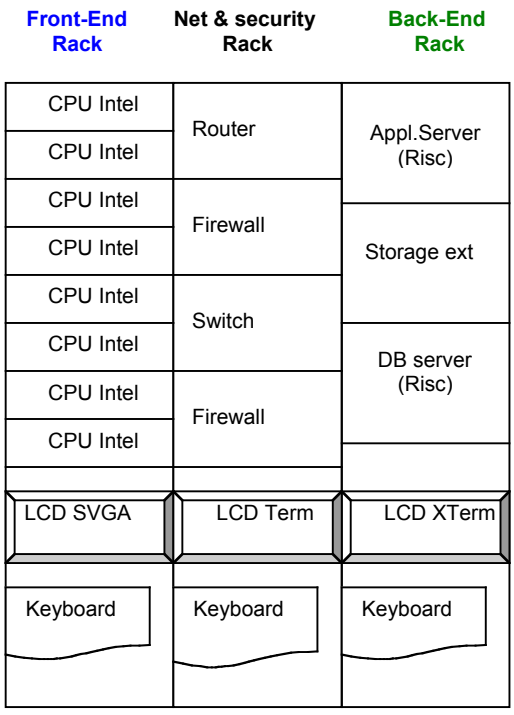


Figura 7 - Gruppo Armadi di una delle due parti del CEST

In ogni armadio sono concentrati apparati della stessa famiglia tecnologica, i cui dispositivi di controllo locale (monitor e tastiera) sono dello stesso tipo, in modo da utilizzare un'unica console per gestire direttamente gli apparati. I diversi tipi di console sono:

- Monitor Super VGA e tastiera per PC per l'armadio che contiene i server Intel
- Monitor di tipo terminale asincrono e relativa tastiera per l'armadio che contiene gli apparati di rete
- Monitor di tipo X-Terminal e relativa tastiera per l'armadio che contiene i server RISC UNIX

Tutti i monitor sono di tipo LCD e tutte le tastiere sono di dimensioni ridotte speciali perché ogni gruppo Monitor-Tastiera (e relativi mouse) è montato su cassetto estraibile che consente ai tecnici di estrarli ed utilizzarli, sedendosi davanti, solo quando necessario.

L'armadio degli apparati di comunicazione è montato in posizione centrale per facilitare le connessioni di rete.

9 Progetto impiantistico del CEST

Il progetto impiantistico definisce in modo accurato come l'infrastruttura tecnologica descritta si inserisce nel contesto del Parco Scientifico Tecnopolis, destinato ad ospitarlo, sfruttandone in modo sinergico le peculiarità di configurazione fisica e di dotazione impiantistica, al fine di garantire gli obiettivi indicati con un minimo sforzo di tipo impiantistico.

Si è già detto che uno dei principali obiettivi è quello di raggiungere un elevato *uptime*, il che comporta la necessità di realizzare una configurazione che non si arresti a fronte di un singolo guasto, classificabile a più livelli, dalla banale interruzione di energia elettrica a eventi di tipo più disastroso quali p. es. incendi.

Questo obiettivo lo si vuole raggiungere in buona sostanza duplicando integralmente il CEST, allocando le sue due parti risultati (Lato-A e Lato-B negli schemi precedenti) in due distinti edifici del Parco Scientifico Tecnopolis.

I due edifici individuati sono, con riferimento alla pianta del Parco nella figura seguente, gli edifici A e H. Essi risultano distanti, circa 500mt., e funzionalmente indipendenti dal punto di vista elettrico in quanto, pur essendo se collegati alla stessa cabina di trasformazione dell'ENEL, sono dotati ognuno di distinti impianti di continuità elettrica a batteria ed a generatore autonomo a gasolio, tali da garantirne l'autonomia indipendente in caso di caduta della rete elettrica primaria e/o di guasto su l'impianto interno dell'altro edificio.

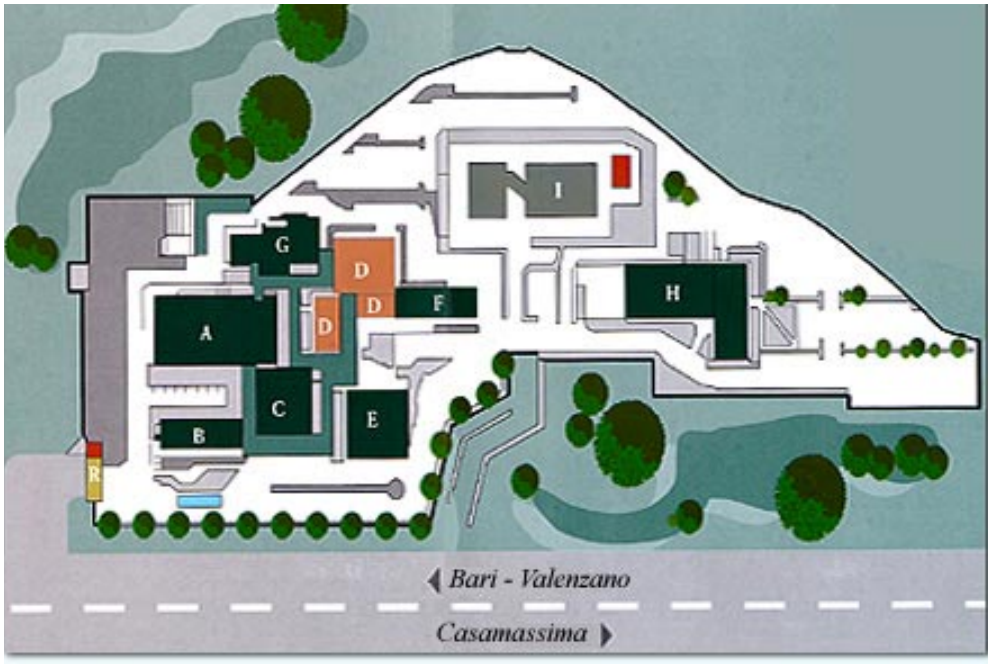


Figura 8 - Pianta del Parco Scientifico Tecnopolis

Peraltro i due edifici sono dotati anche di autonomi impianti ausiliari, quali impianti di rilevazione incendi e di sorveglianza di sicurezza (telecamere a circuito chiuso).

Va sottolineato inoltre che i due edifici sono connessi a livello di rete dati da fasci di fibre ottiche che consentono di instradare le connessioni ad alta velocità tra le parti A e B del CEST senza penalizzazioni dovute alla distanza.

La disponibilità attuale di fibre ottiche di giunzione tra i due edifici è di n.24 Fibre multimodali graded index 62,5/125 micron e n.8 fibre monomodali 9/125 micron.

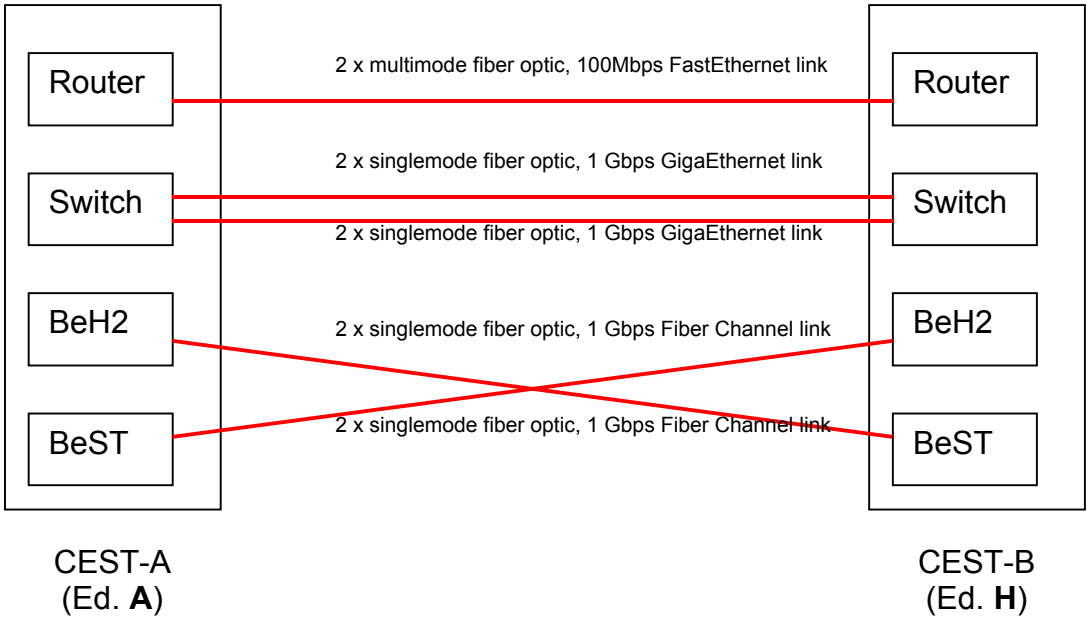


Figura 9 - Utilizzo Fibre Ottiche su dorsale

Per il riferimento ai collegamenti in fibra ottica necessari, si ricava che il fabbisogno iniziale del CEST è di:

- n.2 fibre ottiche multimodali
- n. 8 fibre ottiche monomodali

Che risulta coperto dall'attuale disponibilità di fibre ottiche libere sulla dorsale di campus del Parco Scientifico.

L'allocazione del CEST nei due edifici è prevista come segue:

- nell'edificio A all'interno del CED già esistente (piano terra);
- nell'edificio H, al primo piano in due ambienti prospicienti il locale tecnico esistente di raccordo della rete di Parco.

In entrambi i casi si rende necessaria l'esecuzione di alcuni lavori di adeguamento di tipo logistico per migliorare la garanzia della sicurezza fisica, ferma restando la possibilità di riutilizzare i grandi impianti già esistenti come:

- alimentazione elettrica con UPS e generatori di energia
- dorsali in fibra ottica
- condizionamento
- servizio telefonico
- rilevazioni fumi
- sorveglianza

I lavori di adeguamento (Lotto 4) che si rendono necessari concernono soprattutto la destinazione di ambienti o di parte di essi al servizio dedicato per la RUPAR, attivando su di essi specifici meccanismi di sicurezza e di controllo degli accessi.

10 I costi

La seguente tabella fornisce l'elenco sintetico degli investimenti necessari, suddivisi nei singoli lotti, per la realizzazione del CEST e dei servizi connessi (EPO-LP e CIFRA); i valori espressi potranno essere utilizzati come riferimenti per gli importi a base delle procedure di acquisizione.

Lotto1: Server Intel	**176.299**
Lotto2: Rete e sicurezza	**617.897**
Lotto3: Sistemi centrali di elaborazione e middleware	**640.145**
Lotto4: Adeguamento sicurezza CEST	**20.000**
Lotto5: Potenziamento servizio CIFRA	**67.412**
TOTALE INVESTIMENTO ?	**1.521.753**

Tabella 3 - Riepilogo sintetico dell'investimento

L'investimento, calcolato sulla base dei costi di listino, ammonta a circa 1,5M€. Questi valore è pienamente congruente con quanto previsto nella Convenzione del Centro Tecnico che prevede investimenti per £. 3.450.000.000, pari a Euro 1.781.776.

La quota risultante di Euro. 260.000 costituirà, unitamente agli eventuali risparmi conseguibili in sede di aggiudicazione delle forniture, una riserva da cui poter attingere per eventuali piccoli aggiustamenti/miglioramenti in corso d'opera.

Tecnopolis CSATA

Regione Puglia

Rete Unitaria della Pubblica Amministrazione Regionale

(R.U.P.A.R)

Capitolato Tecnico del Servizio di Trasporto ed Interoperabilità di base

(prodotto nell'ambito della Convenzione approvata dalla Giunta Regionale con deliberazione n. 1162 del 10/8/2001)

Allegato C

Versione 2.1 del 5/8/2002

INDICE

1 Introduzione

Gli scopi, le modalità realizzative, le modalità di finanziamento e le specificazioni tecniche relative alla costituenda RUPAR sono contenute nel documento “Piano Strategico di Sviluppo” della RUPAR-Puglia, che costituisce la premessa indispensabile alla comprensione del quadro d’insieme.

Va precisato tuttavia che per qualsiasi discordanza formale o sostanziale si dovesse eventualmente riscontrare tra il documento “Piano Strategico di Sviluppo della RUPAR” ed il presente Capitolato Tecnico, comprensivo degli Allegati che ne fanno integralmente parte, l’unico riferimento valido ai fini dell’espletamento della gara di selezione è quanto contenuto nel presente Bando.

Il Fornitore di Servizi RUPAR (FSR) deve fornire due servizi come sono stati definiti nel Piano Strategico di Sviluppo:

1. Servizio di Trasporto
2. Servizio di Interoperabilità di Base

e di conseguenza erogherà entrambi i servizi alle Amministrazioni che dovessero rivolgersi a lui per ottenere il Servizio RUPAR, denominazione quest’ultima che nel seguito del presente documento indicherà entrambi i servizi.

2 Specificazione tecnica del Servizio di Trasporto

2.1 Requisiti tecnologici

Il Servizio di Trasporto deve garantire alle Amministrazioni la possibilità di collegare il proprio dominio (Intranet) a quello della RUPAR secondo le specifiche previste dal presente documento.
Il servizio di trasporto è fornito da un FSR selezionato che ha la responsabilità di garantire l'interconnessione con gli altri FSR selezionati.
Tale interconnessione è prevista unicamente in tecnologia TCP/IP come successivamente specificato e quindi si intende per FSR il Fornitore che gestisce l'interconnessione dell'Ente a livello TCP/IP, indipendentemente dai supporti trasmissivi di livello inferiore al protocollo IP che esso utilizza e che può acquistare/noleggiare da un qualsiasi fornitore di servizi di telecomunicazione regolarmente operante in Italia in base a licenza/autorizzazione concessa dal Ministero delle Poste e Telecomunicazioni.

I FSR devono specificare nella risposta al presente Bando il costo per ognuno dei servizi di trasporto previsti nel presente Capitolato Tecnico.

Ogni Amministrazione deve collegarsi a RUPAR mediante i servizi di un unico FSR e non può dotarsi di ulteriori collegamenti a Internet.

Il Servizio di Trasporto della RUPAR si basa su cinque punti di interconnessione tra FSR definiti EPO-LP (Exchange Point Operator, Locale Privato), uno per ogni capoluogo di provincia, gestiti direttamente dal Centro Tecnico.

Un EPO-LP della RUPAR è costituito da un armadio per apparati di comunicazione contenente uno switch Fast/Gigabit Ethernet ad alte prestazioni.
Allo switch si interconnettono i router dei FSR che operano in quella provincia: i router saranno ospitati all'interno dell'armadio.

Ogni FSR ha diritto di allocare nell'armadio del EPO-LP un solo router dotato di una scheda Fast/Gigabit Ethernet, che lo collega allo switch, e di una scheda per connessione a linea geografica, che lo collega al resto della rete del FSR e, per suo tramite, alle Amministrazioni sue clienti.

L'accesso all'armadio del EPO-LP e la gestione dello switch sono di competenza del CT che supervisionerà anche il funzionamento dell'intero EPO-LP controllando l'interscambio di informazioni tra i router, che saranno gestiti ognuno dal proprio FSR.

La scelta del collegamento al EPO-LP in Gigabit Ethernet o in Fast Ethernet è lasciata al FSR che la farà in dipendenza del volume complessivo del traffico scambiato nel EPO-LP e del rispetto dei requisiti sulla Banda Minima Garantita enunciati nel seguito del presente documento.

Le regole cui i FSR si devono uniformare sono le seguenti:

1. esistono **cinque** EPO-LP, uno per ogni provincia, ognuno dei quali supporta il traffico di interscambio tra i FSR per gli Enti localizzati in quella provincia;
2. lo EPO-LP di Bari ha funzioni anche di interscambio interprovinciale e di backup degli altri EPO-LP in caso di loro guasto;
3. ogni FSR deve essere sempre interconnesso a tutti gli EPO-LP;

4. per la corretta operatività degli EPO-LP i FSR dovranno disporre di un adeguato numero di reti ufficiali di classe C riservate al solo servizio RUPAR, per la gestione degli indirizzi delle Amministrazioni clienti, ed infine utilizzare il protocollo BGP-4 per il routing negli EPO-LP;
5. il routing BGP-4 che verrà effettuato negli EPO-LP concernerà esclusivamente le reti **riservate** (la cui assegnazione è controllata dal CT per la parte Extranet della RUPAR) e pubbliche (reti di classe C di proprietà dei FSR e riservate alla RUPAR) che verranno definite come appartenenti ad Autonomous System privati (AS numeri da 64512 a 65535, cfr. RFC1930);
6. la gestione dell'instradamento dovrà essere *Classless* (CIDR, Classless Inter Domain Routing);
7. gli stessi FSR dovranno poi annunciare le reti pubbliche di classe C di propria pertinenza per il servizio RUPAR sull'Internet nazionale ed internazionale mediante la propria connessione ad Internet ed i propri Autonomous System ufficiali;
8. deve esistere un disaccoppiamento tra il routing BGP-4 privato della RUPAR ed il routing a livello di Internet: questo risultato può essere ottenuto da un FSR semplicemente annunciando in modo statico nella propria rete globale connessa a Internet, la parte ufficiale della rete RUPAR di propria pertinenza;
9. non sono ammesse politiche di "source-routing";
10. lo EPO-LP di Bari sarà allocato presso il Centro Tecnico e strettamente interconnesso alla sua infrastruttura tecnologica. La sua caratteristica saliente sarà quella di essere **completamente ridondato**; saranno, quindi, disponibili n.2 armadi EPO-LP contenenti

ognuno uno switch di interconnessione, allocati a circa 500 m. di distanza e collegati in fibra ottica;

11. gli EPO-LP provinciali saranno ubicati, in ambito urbano, nelle città di Foggia, di Brindisi, i Taranto e di Lecce.

Oltre a queste regole che concernono il funzionamento stesso della rete e dei protocolli di instradamento, si prevede che i FSR debbano uniformarsi alle seguenti regole di gestione:

1. tutti i router dei FSR devono consentire l'accesso in sola lettura via protocollo SNMP da parte del sistema centrale di controllo del CT, il cui indirizzo verrà comunicato allo FSR al momento dell'abilitazione ad operare: il sistema centrale di controllo del CT farà uso, oltre che del protocollo SNMP, anche del protocollo ICMP;
2. i router della RUPAR dovranno essere sincronizzati al Tempo Ufficiale di Rete che verrà propagato nella RUPAR a cura del CT;
3. i router di un FSR che svolgono servizio RUPAR dovranno essere riservati alla RUPAR e non potranno essere utilizzati per servire altri utenti;
4. ogni FSR dovrà consentire, qualora reputato necessario dal CT, l'installazione di *probe* (sonde di traffico) sugli switch dei EPO-LP al fine di monitorare il traffico scambiato nel EPO-LP;
5. ogni FSR deve attivare un proprio **Centro di Gestione** (**CG-FSR**) attivo 365 giorni l'anno h24, con un numero telefonico a disposizione dei propri utenti ed un'altro a disposizione del CT e degli altri Centri di Gestione. Il CG-FSR è tenuto a collaborare con il CT e con gli altri Centri di Gestione al fine di eliminare

qualsiasi malfunzionamento della rete e di consentire l'ottimizzazione del traffico.

La versione dell'IP che deve essere inizialmente supportata è la versione 4.

La modalità tecniche di erogazione del Servizio di Trasporto concernono inoltre le modalità di instradamento del traffico (*routing*).

Le principali regole concernenti il routing sono le seguenti:

1. ogni FSR deve realizzare negli EPO-LP cui è collegato sessioni di peering BGP-4 privato con tutti gli altri fornitori; su queste sessioni deve essere scambiato traffico concernente esclusivamente le reti RUPAR;
2. le reti RUPAR apprese da un FSR negli EPO-LP, non devono essere propagate nella propria infrastruttura al di là della parte che contiene le utenze RUPAR; il traffico di utenti non RUPAR collegati ad un FSR verso Enti RUPAR collegati mediante altro FSR deve seguire il normale flusso sul backbone Internet nazionale per transitare sulla rete dell'altro FSR;
3. le reti di classe C di un FSR, corrispondenti agli Enti gestiti da quel FSR in una specifica provincia, annunciate via BGP-4 nel EPO-LP della Provincia e in quello di Bari sono apprese dagli altri FSR nel EPO-LP della Provincia e in quello di Bari. Poiché lo EPO-LP di Bari ha la funzione di backup degli EPO-LP provinciali, è opportuno che i FSR gestiscano in modo dinamico instradamenti multipli e variabili nel tempo.

2.2 Definizione dei servizi e dei parametri per l'offerta economica

E' stato già definito che l'interconnessione dei FSR è basata esclusivamente sul protocollo IP, ma ovviamente essi realizzeranno il servizio mediante circuiti portanti di tecnologia diversa.

In generale i FSR potranno offrire tutti i servizi di telecomunicazione basati su circuiti portanti di cui sia ammessa dalla legislazione vigente la vendita al pubblico con l'unica restrizione che il tipo di collegamento richiesto tra la sede dell'Amministrazione utente e la rete RUPAR è sempre di tipo permanente, escludendo quindi, salvo i casi particolari di seguito descritti, l'utilizzo di collegamenti di tipo commutato quali la Rete Telefonica Generale (RTG, di tipo analogico) e la rete ISDN.

Sono quindi da considerare tra i collegamenti di tipo:

- CDN (linea affittata anche di tipo parziale)
- xDSL (varie tipologie, ADSL, HDSL etc.)
- WLL/FA (Wireless Local Loop/Fixed Access)

Nella risposta al Bando deve essere offerto il Servizio di Trasporto per una gamma di velocità di accesso (velocità della linea di collegamento dell'Amministrazione con il nodo della rete RUPAR gestito dal Fornitore), **distinguendo i due casi** di Amministrazione utente allocata in **Provincia di Bari** e Amministrazione utente allocata in **altra Provincia**. Le velocità previste, sempre per collegamenti permanenti, bidirezionali simmetrici, sono le seguenti:

Servizio di Trasporto		
	Servizio in Provincia diversa da Bari	**Servizio nella Provincia di Bari**
	€/Anno	*€/Anno*
64	$T_{64\text{-}PR}$	$T_{64\text{-}BA}$
128	$T_{128\text{-}PR}$	$T_{128\text{-}BA}$
256	$T_{256\text{-}PR}$	$T_{256\text{-}BA}$
384	$T_{384\text{-}PR}$	$T_{384\text{-}BA}$
512	$T_{512\text{-}PR}$	$T_{512\text{-}BA}$
768	$T_{768\text{-}PR}$	$T_{768\text{-}BA}$
2048	$T_{2048\text{-}PR}$	$T_{2048\text{-}BA}$

Tabella 1 - Classi di servizio di accesso a RUPAR

Il valore del servizio che dovrà essere indicato nell'offerta **dovrà** essere privo del costo della linea di collegamento fisico dell'Amministrazione al nodo del Fornitore; questo costo sarà valutato in modo indipendente dall'effettiva tecnologia realizzativa del collegamento sulla base dell'Offerta di linee affittate Wholesale della Telecom Italia come prevista dalla Delibera n. 59/02/CONS dell'Autorità Garante per le Comunicazioni (AGCOM).
Saranno ammissibili anche circuiti di tipo asimmetrico (p. es. ADSL a varie velocità 128/640 Kbps o 512/2048 Kbps) purché l'Amministrazione richiedente la giudichi una soluzione idonea alle proprie necessità e fermo restando che la quota parte di finanziamento prevista a carico della Regione Puglia sarà comunque pari al 50% del valore del Servizio di Trasporto e del circuito di collegamento bidirezionale così come precedentemente specificato.

Per quanto concerne i collegamenti di tipo commutato (ISDN o RTG, Rete Telefonica Generale), essi **devono** essere resi disponibili dal Fornitore se non

sono tecnicamente attivabili altri tipi di collegamento ed in questo caso dovranno essere realizzati aggregando canali telefonici in modo da raggiungere la velocità di collegamento prevista. Deve essere considerata primariamente la possibilità di fornire un collegamento alternativo di tipo ISDN e, solo nel caso in cui questo non fosse disponibile, deve essere fornito un collegamento via RTG, dello stesso numero di canali telefonici del caso ISDN: si equipara qui un canale telefonico RTG ad uno ISDN.

Oltre che nel caso di indisponibilità di collegamenti dati permanenti, un collegamento di tipo commutato è ammissibile se la stessa Amministrazione richiedente lo predilige per un qualsiasi motivo, resta ferma in ogni caso che la quota parte di finanziamento prevista a carico della Regione Puglia sarà comunque pari al 50% del valore del Servizio di Trasporto e del circuito di collegamento bidirezionale così come precedentemente specificato.

Poichè il Servizio di Trasporto in RUPAR è un servizio IP, i FSR sono liberi di utilizzare all'interno della loro parte di rete l'incapsulamento dell'IP in protocolli di trasporto quali HDLC, PPP, Frame Relay o ATM ovvero protocolli proprietari.

L'incapsulamento dell'IP nei EPO-LP è obbligatoriamente in frame Ethernet con velocità 100/1000 Mbps; l'incapsulamento dell'IP nel punto di interconnessione dall'Amministrazione, per collegamenti di tipo permanente, è obbligatoriamente in frame Ethernet con velocità 10/100 Mbps su connettore RJ45: la scelta della velocità di quest'ultimo collegamento sarà di esclusiva pertinenza dell'Amministrazione senza variazioni di costo.

Per i collegamenti di tipo commutato (linea telefonica analogica e ISDN) il protocollo IP deve essere incapsulato in frame PPP (Point to Point Protocol, RFC 1661 e seguenti) con il supporto dell'aggregazione dei canali (Multilink PPP, RFC 1717 e seguenti) per le velocità multiple di un canale base ISDN.
Nei collegamenti di tipo commutato, l'autenticazione dell'utente dovrà avvenire mediante un protocollo che prevede la **crittografia** della password.

Dopo l'autenticazione dovrà essere assegnato all'utente un **indirizzo IP statico**, sempre lo stesso per tutti i collegamenti successivi; se il tipo di rete utilizzata lo consente (rete digitale) deve essere anche vincolato il numero di telefono chiamante autorizzato.

Inoltre deve essere garantita la funzionalità di "CallBack" per cui il circuito commutato è dal punto di vista funzionale equivalente ad un circuito permanente, dato che l'attivazione della connessione telefonica può avvenire sia per una richiesta proveniente dalla rete dell'Amministrazione di poter raggiungere una qualsivoglia destinazione esterna, sia per una richiesta proveniente dalla rete RUPAR di poter raggiungere la rete dell'Amministrazione.
Sempre al fine di rendere il più possibile equivalente un circuito commutato ad uno permanente e quindi per minimizzare l'effetto di ritardo dovuto all'instaurazione della connessione telefonica si richiede che il parametro di abbattimento automatico della connessione, individuato dal tempo trascorso in condizioni di totale assenza di traffico, sia non inferiore a 10' (minuti) per la rete ISDN e non inferiore a 30' (minuti) per la RTG.

Sul collegamento della rete di dominio dell'Amministrazione con la rete del FSR, dovranno essere garantiti i livelli di servizio di trasporto e specificatamente la Banda Minima Garantita (BMG) verso i quattro seguenti principali snodi di trasporto, che tipicamente sono raggiungibili attraverso altrettanti circuiti virtuali:

1. **all'EPO-LP provinciale** (*BMG-Prov* = 1° frazione della velocità della linea di collegamento al FSR);
2. **all'EPO-LP regionale** (*BMG-Reg* = 2° frazione della velocità della linea di collegamento al FSR);
3. **a Internet nazionale** (*BMG-Naz* = 3° frazione della velocità della linea di collegamento al FSR);
4. **a Internet internazionale** (*BMG-Int* = 4° frazione della velocità della linea di collegamento al FSR).

Le somma delle quattro BMG può essere superiore ad 1, intendendo ovviamente che quei valori non siano ottenuti simultaneamente, in ogni caso deve essere garantito che, in assenza di traffico sulle altre direttrici, il traffico su una specifica direttrice possa raggiungere almeno il valore richiesto.
Per ognuna delle classi di servizio indicate in Tabella 1 il livello di servizio che deve essere previsto nell'offerta, relativamente alla velocità di linea (VdL), è il seguente:

- BMG-Prov = 75% VdL
- BMG-Reg = 50% VdL
- BMG-Naz = 50% VdL
- BMG-Int = BMG-Naz

Per ognuna delle **classi di servizio** di Tabella 1 dovranno essere indicati due costi:

1. il costo relativo al collegamento delle Amministrazioni della provincia di Bari;
2. il costo relativo al collegamento delle Amministrazioni di una qualsiasi delle altre province.

Ognuno di essi dovrà essere un costo:

- **omnicomprensivo**, ivi inclusi tutti i servizi di supporto richiesti nel presente capitolato tecnico e l'utilizzo di tutte le apparecchiature necessarie (Router, modem etc.) per fornire il trasporto tra i due incapsulamenti del protocollo IP specificati come obbligatori: presso l'Amministrazione e nell'EPO-LP di pertinenza;
- **indipendente dalla distanza** dell'Amministrazione dall'EPO-LP provinciale: si ribadisce che **non** deve contenere il costo della linea di collegamento;
- di tipo "***flat***" (canone annuo), indipendente sia dal tempo in cui l'Amministrazione trasmette o riceve traffico sia dal volume del traffico stesso;
- **privo di voci una-tantum** (p. es. attivazione).

2.3 Standard tecnici di riferimento

Il Servizio di Trasporto, così come definito nel presente documento, si attua a livello RUPAR, e quindi negli EPO-LP, esclusivamente mediante il protocollo IP.
Devono quindi essere rispettati tutti gli standard tecnici relativi ai protocolli TCP/IP, tuttavia poiché è richiesto che i FSR rendano disponibili circuiti di accesso alla RUPAR basati sui servizi di comunicazioni la cui vendita al pubblico è ammessa dalla normativa vigente, ne consegue che anche gli standard tecnici che regolamentano tali servizi di comunicazione sono vincolanti per i FSR.

Sono vincolanti sia gli standard "*de jure*" emessi da Enti pubblici nazionali e internazionali, sia da standard "de facto" governati da Enti privati ("Forum") costituiti da accordi industriali dei fornitori delle specifiche tecnologie. Sono di seguito specificati gli Enti i cui standard devono essere rispettati per le specifiche tecnologie.

2.3.1 Standard TCP/IP

Gli standard tecnici di riferimento relativi ai protocolli TCP/IP sono quelli emanati dal competente Centro di gestione tecnica della rete Internet: IETF (Internet Engineering Task Force: URL: http://www.ietf.org).

In generale e' richiesto ai FSR di adottare gli standard tecnici una volta emanati dall'IETF, solo in qualche caso eccezionale potrà essere avviata dal CT una procedura per arrivare all'adozione anticipata, con il consenso di tutti i

Fornitori interessati, di uno standard ancora in via di approvazione definitiva da parte dello IETF.

Lo standard IETF è in genere specificato mediante la sigla RFC (Request For Comment) del documento che lo specifica, il quale va considerato unitamente agli eventuali documenti successivi che lo rendono obsoleto, modificandolo e integrandolo.

Poiché l'interazione tra diversi fornitori a livello RUPAR si realizza nei EPOLP, è di fondamentale importanza il supporto del protocollo BGP-4 (RFC1771, "A Border Gateway Protocol") e della gestione dell'aggregazione degli indirizzi CIDR (RFC1519, "Classless InterDomain Routing").

2.3.2 Standard dei servizi di comunicazioni

Per ognuno dei servizi di comunicazioni supportati sono rilevanti, oltre agli standard prescritti dal regolamento tecnico del servizio come approvato dal competente Ministero, gli standard dell'IETF che specificano le modalità del trasporto del TCP/IP sul servizio in questione: p. es. PPP (RFC1661, "Point to Point Protocol") per il trasporto su linee seriali e MPPP (RFC1717, "Multilink PPP") per l'aggregazione di più link in parallelo per realizzare un unico collegamento a velocità più elevata.

In generale per le tecnologie di trasmissione a livello locale e geografico sono rilevanti gli standard emessi da:

- IEEE (Institute of Electrical and Electronics Engineers, URL: http://www.ieee.org) normalmente recepiti dall'ISO (International Standard Organization, URL: http://www.iso.ch);

- ETSI (European Telecommunication Standard Institute, URL: http://www.etsi.org);
- ITU-T (International Telecommunication Union-Telecom, URL: http://www.itu.int/ITU-T/);
- ATMForum (URL: http://www.atmforum.com);
- FrameRelayForum (URL: http://www.frforum.com).

Hanno inoltre valore vincolante le prescrizioni emesse mediante propria delibera dall'Autorità Garante delle Comunicazioni (AGCOM).

2.3.3 La Qualità tecnica del servizio

La qualità tecnica del Servizio di trasporto si misura mediante le seguenti metriche:

1. disponibilità del servizio;
2. prestazioni dei collegamenti.

La disponibilità del servizio è misurata in base ai due parametri di Uptime (Tempo ininterrotto di disponibilità di un servizio) e MTBF (Mean Time Between Failures, tempo che intercorre tra due guasti consecutivi dello stesso servizio).

La disponibilità di base richiesta è di 24 ore al giorno e 365 giorni l'anno.

I valori richiesti sono i seguenti:

1. Uptime > 99,5%
2. MTBF > 2000 ore

Si noti che il parametro di Uptime è comprensivo anche degli interventi, con caratteristiche bloccanti del servizio, programmati per finalità di manutenzione preventiva e/o evolutiva.

Per tutti i servizi si richiede che eventuali interruzioni di servizio per manutenzioni siano comunicate con un anticipo di almeno 3 giorni.

Per le prestazioni dei collegamenti i due parametri fondamentali sono il rispetto della BMG (Banda Minima Garantita) e il tasso di perdita di pacchetti.

Utilizzando come unità campione una sequenza (> 10) di pacchetti Ping (ICMP Echo) di dimensione 8000 bytes, la verifica dei parametri consiste nella rilevazione, per tutti i circuiti virtuali su cui sia garantita una BMG, delle seguenti grandezze:

1. **RoundTripDelay** < C*128/BMG sec (dove C=1,2 per il collegamento all'EPO-LP provinciale e C=1,5 per gli altri; il RoundTripDelay è il tempo di risposta medio fornito dallo strumento/comando "**ping**" espresso in secondi; la BMG è espressa in Kbit/sec)
2. **Tasso di perdita** < 0,1%
3. **Tempo di download/upload** < C*8*DimensioneFile/BMG sec. (C=1,2 DimensioneFile è espressa il Kbytes e la BMG in Kbit/sec).

Per i collegamenti di tipo commutato si richiede inoltre che siano previsti nel nodo di rete un numero di canali telefonici pari a quello delle Amministrazioni collegate, in modo che la probabilità di trovare la linea occupata sia nulla.

3 Specificazione tecnica del Servizio di Interoperabilità

3.1 Requisiti tecnologici

Il **Servizio di Interoperabilità** deve garantire alle Amministrazioni la possibilità di collegare il proprio dominio (Intranet) a quello della RUPAR secondo le specifiche previste dal presente documento.

Il Servizio di Interoperabilità è fornito da un FSR selezionato che ha la responsabilità di garantire lo scambio di informazioni con gli altri FSR selezionati, con altri Domini Amministrativi e con Internet. Considerando la univocità del FSR per la singola Amministrazione, il FSR dovrà attrezzare impianti di erogazione conformi per eventuali servizi aggiuntivi richiesti dalle Amministrazioni.

Il Dominio di ciascuna Amministrazione dovrà usufruire dei Servizi di Interoperabilità attraverso un solo Punto di Accesso ai Servizi di Interoperabilità, definito **Porta di Rete** (**PdR**) come unico elemento logico dove risiedono le funzionalità di Firewall e di proxy per i servizi applicativi.

Il FSR deve essere un fornitore di servizi e prodotti di comunicazione telematici, interattivi e multimediali regolarmente operante in Italia in base a licenza/autorizzazione concessa dal Ministero delle Poste e Telecomunicazioni.

Ogni Amministrazione collegandosi a RUPAR, attraverso la PdR, deve utilizzare i servizi di interoperabilità previsti dal suo unico FSR.

Ogni FSR deve predisporre un servizio di interoperabilità che abbia funzionalità di base ed in particolare:

a. Domain Name System
b. Directory
c. Tempo ufficiale di rete
d. Gestione sistemi e rete
e. Sicurezza

e funzionalità applicative, intendendo in particolare:

f. Posta Elettronica
g. Accesso a WWW
h. Trasferimento file
i. Terminale virtuale
j. Accesso a news

L'Amministrazione può richiedere al FSR dei servizi aggiuntivi come:

k. servizi di *housing* e *mirroring* di servizi/siti web
l. servizi di collegamento a banche dati esterne di interesse generale
m. servizi di gestione interna all'Amministrazione
n. servizi di outsourcing per sistemi informativi presenti all'interno

Il CG-FSR, già definito per i Servizi di Trasporto, dovrà svolgere anche le funzioni di Centro di Gestione per l'Interoperabilità, che deve essere considerato parte integrante del progetto offerto e può coincidere con il Centro Servizi, eventualmente predisposto dal FSR per erogare servizi di interoperabilità a distanza rispetto al PdR.

Il Fornitore, nell'ambito della propria organizzazione, condurrà le operazioni in maniera da:

1. minimizzare la probabilità di intercettazione, accesso, modifiche, distruzione non autorizzate o l'uso improprio relativamente alle informazioni degli utenti in transito nel Dominio della Rete unitaria regionale;
2. minimizzare la probabilità di accesso, comunicazione, modifiche, distruzione non autorizzate o uso improprio delle informazioni delle Amministrazioni comunque residenti negli apparati gestiti dal CG-FSR, nel Centro servizi e nella Struttura di Gestione per i Servizi Addizionali.

Il Centro Tecnico può adeguare le prescrizioni minime di sicurezza contenute nel presente Capitolato:

- al verificarsi di variazioni del livello di rischio cui sono soggetti i servizi o i dati delle Amministrazioni;
- a seguito di modifiche della tecnologia informatica utilizzata per erogare i servizi;
- in caso di disponibilità di tecnologie più evolute nell'ambito della sicurezza.

Il Fornitore è tenuto a mantenere aggiornato il sistema di sicurezza rispetto a tali revisioni.

In generale, il Servizio per l'Interoperabilità della RUPAR può essere erogato in diversi punti della rete unitaria regionale; in particolare il singolo FSR può erogare i servizi in tre modi:

1. in modo totalmente centralizzato mediante uno o più propri Centri Servizi connessi a RUPAR a cui le Amministrazioni clienti si collegano in modo trasparente;
2. in modo distribuito mediante l'allocazione di risorse elaborative presso la connessione in RUPAR delle Amministrazioni;
3. in modo misto, con alcuni servizi allocati presso le Amministrazioni ed altri centralizzati.

L'unica risorsa elaborativa che deve sempre essere allocata presso l'Amministrazione è il Proxy/Firewall installato nella PdR.
Il Firewall deve garantire la sicurezza della Intranet dell'Amministrazione e può prevedere sia una zona demilitarizzata DMZ che una Rete dei Servizi RUPAR (RSR), rispettivamente per l'ospitalità di sistemi di erogazione di pubblica utilità (per il cittadino) e quelli riservati RUPAR; in questa configurazione il Firewall ha quattro interfacce di rete:

1. rete interna
2. rete DMZ
3. rete RSR
4. rete esterna

In tutti i casi, il FSR resta il responsabile della erogazione della totalità dei servizi di interoperabilità previsti, nonché del supporto (indirizzamento, nomi e sicurezza a livello Firewall) dei servizi applicativi che dovessero essere attivati dall'Amministrazione sull'infrastruttura dei servizi di interoperabilità di base.

Per meglio disciplinare i casi di attacchi fisici, di danneggiamenti involontari o dolosi alla strumentazione (Firewall, hub Ethernet, etc.) si richiede che gli

apparati della PdR, a cura del FSR, siano installati in armadi metallici predisposti in aree rese disponibili dall'Amministrazione. Gli armadi muniti di serratura dovranno essere acceduti esclusivamente da personale del FSR. Il rischio di scasso dovrà essere scongiurato dal sistema di sorveglianza dell'Amministrazione.
Il FSR, comunque, è sempre il responsabile dell'attuazione delle politiche di sicurezza verso la RUPAR e le reti esterne per l'Amministrazione.

Il FSR dovrà assicurare al Centro Tecnico ed alle Amministrazioni, a ciascuno per quanto di propria competenza, strumenti per il controllo dello stato di funzionamento dei Servizi per l'Iteroperabilità, inoltre dovrà prevedere una documentazione completa e ufficiale per la verifica e l'analisi dei servizi erogati presso la PdR, sulla base del traffico applicativo registrato. Il FSR indicherà gli strumenti per il controllo in tempo reale dello stato di funzionamento ed il contenuto dei report periodici.

Le regole cui i FSR si devono uniformare sono le seguenti:

1. Ogni FSR dovrà garantire la sicurezza dei servizi erogati;
2. I server della RUPAR dovranno essere sincronizzati al Tempo Ufficiale di Rete che verrà propagato nella RUPAR a cura del CT;
3. I server di un FSR che svolgono servizio RUPAR (connessi alla rete RSR - Rete delle Risorse RUPAR) dovranno essere riservati alla RUPAR e non potranno essere utilizzati per servire altri utenti;
4. Ogni FSR dovrà consentire, qualora reputato necessario dal CT, l'installazione di probe (sonde di traffico) sugli switch delle reti LAN presenti nel PdR e/o nel Centro di Gestione per l'Interoperabilità.

3.2 Descrizione dei servizi di interoperabilità di base

Per ogni servizio si indica il livello base di erogazione, il cui costo è compreso nel valore dell'offerta ed il livello opzionale, che può essere richiesto dalle Amministrazioni, con il relativo costo a loro carico e deve essere erogato.

3.2.1 Gestione dei Nomi di Dominio (DNS)

Consiste nella gestione del dominio che identifica l'Amministrazione nonchè di tutti i nomi degli elaboratori sulle reti di servizio (DMZ e RSR).

Il livello base di erogazione del servizio prevede l'allocazione degli elaboratori che gestiscono la risoluzione dei nomi gestiti dal FSR presso il Centro Servizi del FSR.
L'allocazione di almeno uno degli elaboratori presso la PdR è servizio opzionale, che può essere richiesto dall'Amministrazione.

Successivamente alla fase di attribuzione, da parte del FST, delle *subnet* di indirizzi IP necessarie al corretto funzionamento degli apparati e delle postazioni di lavoro dell'Amministrazione, il FSR si adopererà per l'attivazione del dominio Internet dell'Amministrazione, oltre che della predisposizione del Proxy/Firewall e degli altri servizi di interoperabilità.
Come già evidenziato in precedenza, a differenza del collegamento Internet (che viene sempre incluso nell'offerta di servizio di trasporto), la singola Amministrazione potrebbe non richiedere immediatamente la predisposizione di una rete DMZ e/o di una rete RSR. Pertanto, nella successiva lista delle funzionalità si dovrà tener conto di questa evenienza.

Recepito dall'Amministrazione il nome del dominio da attivare, il FSR dovrà:

1. garantire la fruizione del servizio di risoluzione dei nomi a tutte le postazioni del Dominio Amministrativo fornendo modalità tecniche di utilizzo;
2. coordinare la gestione del naming per tutte le reti (DMZ, Intranet, RSR); in particolare, per un host raggiungibile da più reti (ad es. dalla rete Intranet della generica Amministrazione e dalla rete Internet) dovrà essere utilizzato sempre lo stesso nome simbolico;
3. su Internet, predisporre il DNS server primario per il nome del dominio individuato dalla Amministrazione; quindi, predisporre almeno un DNS server secondario del precedente primario; nessun nome di host presente sulla Intranet e/o sulla rete RSR dovrà essere incluso in questo database;
4. sulla RSR, garantire la visibilità del DNS di riferimento gestito dal CT, che contiene le risorse RUPAR attivate sulla rete regionale;
5. richiedere indirizzi e nomi di dominio validi prima di predisporre host sulla rete RSR.

Come servizio opzionale appartenente a questa categoria il FSR può, se richiesto dall'Amministrazione, predisporre e gestire il DNS server primario e secondario sulla Intranet per il nome del dominio individuato dalla stessa Amministrazione, predisponendo meccanismi di *forward* per risolvere nomi esterni.

Affinché le postazioni client della Intranet possano utilizzare i servizi di interoperabilità, il FSR dovrà fornire all'Amministrazione indicazioni tecniche coerenti con la configurazione del Proxy/Firewall presente nel PdR.

Per risolvere i nomi degli host afferenti alle reti RSR, il FSR dovrà predisporre all'occorrenza meccanismi di caching/forwarding per indirizzare il DNS delle risorse RSR gestito dal CT.
Nel caso in cui l'Amministrazione chiedesse la predisposizione di una LAN RSR, il FSR si farà carico della registrazione e dell'attivazione tecnica del sottodominio *subdomain*.rupar.puglia.it coordinandosi con il CT, in qualità di gestore del dominio di più alto livello.
La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC1034, RFC1035, RFC2535 e successive estensioni.

3.2.2 Directory

Consiste nella gestione di classi di oggetti accessibili attraverso l'infrastruttura di servizi.

Il livello base di erogazione del servizio prevede l'allocazione degli elaboratori che gestiscono il Servizio di Directory presso il Centro Servizi del FSR.
L'allocazione di almeno uno degli elaboratori presso la PdR è servizio opzionale, che può essere richiesto dall'Amministrazione.

Come set minimo di informazioni, il servizio deve gestire l'anagrafica ed i recapiti telefonici e di email dei dipendenti dell'Amministrazione. Il servizio dovrà essere integrato da informazioni (attributi) pubbliche tipo "public security keys" non appena disponibili.

Il servizio, conforme alle specifiche X.500 e con il supporto del protocollo LDAP, verrà successivamente integrato con la posta elettronica fornendo così una rubrica di indirizzi degli utenti come parte integrante dell'infrastruttura di sicurezza.
Oltre al descritto LDAP server pubblico, al fornitore potrà essere richiesto di attrezzare e gestire un più completo LDAP server RUPAR sulla rete RSR. Mediante opzioni di replicazione parziale del server LDAP RUPAR si aggiornerà il server pubblico sulla rete DMZ.
La documentazione ufficiale (standard) di riferimento è la seguente: RFC1777, RFC2247 e loro aggiornamenti.

3.2.3 Tempo ufficiale di rete

Consiste nel gestire il recepimento del tempo ufficiale propagato dal CT sulla RUPAR e nella sua distribuzione a tutti gli elaboratori di servizio.
L'applicazione software che permetterà alle risorse di comunicazione ed elaborazione collegate alla RUPAR di sincronizzare i propri orologi è il Network Time Protocol versione 3. Il protocollo sarà attivato in modalità sicurizzata per garantire sicurezza e autenticità del tempo.

La sincronizzazione dei clock sarà obbligatoria per tutti gli apparati di instradamento e per tutti gli "host services" mentre per le principali piattaforme client potranno essere impiegate soluzioni software conformi.
Il Time Server NTP primario della RUPAR verrà gestito dal CT presso il EPO-LP di Bari; i FSR sincronizzeranno i clock dei propri dispositivi presenti presso il EPO-LP e daranno origine ad una gerarchia di strati NTP indicati per sincronizzare gli orologi di tutti i dispositivi afferenti alla propria rete di trasporto.

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC1305 e successivi aggiornamenti.

3.2.4 Gestione sistemi e rete

Consiste nella gestione sistemistica e nel monitoraggio di tutti gli apparati di propria competenza che supportano i servizi erogati alle Amministrazioni.
Per l'attività di gestione sistemistica e monitoraggio dei server e dei servizi ospitati, si dovrà prevedere l'utilizzo di soluzioni/metodologie client-server e più specificatamente "agent-manager" basate sullo standard IETF SNMP (Simple Network Management Protocol) ed RMON (Remote network MONitoring).
La gestione riguarderà specificatamente:

- i dispositivi presso la sede della generica Amministrazione (server Proxy, Firewall, host services);
- gli apparati del Centro Servizi (router, concentratori LAN, host services, Firewall).

Sia i FSR dovranno autorizzare sessioni SNMP da/verso Manager SNMP gestiti dal CT.
Le attività di gestione saranno espletate secondo le prescrizioni del capitolo successivo e comunque rispettando gli standard IETF SNMP basate su community string (RFC1157).
Successivamente, potranno essere implementati modelli sicurizzati basati su SNMPv3 (RFC2570, non standard ed appartenente alla categoria "*Informational*").

Oltre ai citati, altri documenti ufficiali (standard IETF) sono: RFC1757 e RFC2021.

3.2.5 Sicurezza

La gestione della sicurezza che compete ai FSR concerne essenzialmente:

1. i Firewall di protezione dei servizi;
2. i sistemi IDS (Intrusion Detection System) addetti alla rivelazione di tentativi complessi di intrusione;
3. i servizi di VPN (Virtual Private Network).

Delle tre funzionalità, per le quali segue la specificazione tecnica, solo la prima è obbligatoria in una versione base che contempla la protezione della sola Intranet dell'Amministrazione, mentre le altre due sono opzionali.
L'attivazione sul Firewall di ulteriori reti da proteggere (DMZ e/o RSR) è servizio opzionale, così come costituisce servizio opzionale la gestione, dal punto di vista dell'indirizzamento, dei nomi e della sicurezza a livello Firewall, di elaboratori posti sulle due reti RSR e DMZ.

I Firewall, sono preposti alla protezione dell'intero accesso all'esterno sia per i servizi che per le stazioni utente. E'essenziale che essi adottino tutte le opportune politiche di protezione come:

- sbarramento statico di tutte le porte applicative non destinate ad erogare servizio, al fine di limitare le possibilità di attacco agli elaboratori preposti all'erogazione dei servizi

- sbarramento statico dell'accessibilità di specifiche reti a partire da altre reti: p. es. limitazione degli accessi ai servizi su reti RSR ai soli indirizzi privati della RUPAR
- filtraggio in tempo reale del traffico con tecniche di ispezione a livello di protocollo (*packet inspection*) ed a livello di dati (*stateful inspection*) al fine di garantire sia l'arresto di attacchi di tipo DOS (Denial Of Service) che il blocco di flussi informativi contenenti minacce di cui si riconosca la "firma" (Virus, Applet Java, Cavalli di Troia etc.)
- mascheramento delle stazioni client (legato al servizio di accesso a WWW o Proxy): si richiede che le stazioni utente dell'Intranet, corrispondenti ai PdL gestiti, possano per default accedere in modalità NAT (Network Address Translation) o PAT (Protocol Address Translation) ai servizi di interoperabilità della RUPAR mediante gli specifici protocolli (SMTP, POP3, LDAP, NNTP etc.) che non siano supportati dal Proxy; si richiede altresì che sia possibile attivare analoghi meccanismi per altri protocolli su richiesta delle Amministrazioni senza che ciò comporti oneri aggiuntivi.; costituisce invece servizio opzionale l'abilitazione selettiva dei suddetti servizi NAT/PAT per singoli PdL; il supporto NAT/PAT deve essere erogato mediante il Firewall sempre in osservanza dei requisiti di sicurezza specificati;
- log delle sessioni per registrare lo sviluppo del traffico gestito.

I sistemi IDS, opzionali, rappresentano un secondo livello di protezione che si caratterizza come segue:

- la loro presenza è ignota ai potenziali aggressori e da loro non rivelabile;

- sono in grado di effettuare analisi sofisticate sul traffico, con metodologie tipiche di sistemi esperti, rivelando attacchi di struttura complessa;
- non rallentano l'attività di inoltro del traffico, dato che operano in modo passivo sulla rete (analisi del traffico in modo promiscuo o "*sniffing*") e non hanno il compito di smistare traffico;
- sono in grado di pilotare il Firewall stesso per attivare in tempo reale sbarramenti rispetto ad indirizzi mittenti individuati come fonte di aggressioni in corso;
- provvedono sia alla registrazione delle anomalie che alla generazione di allarmi verso il personale di gestione.

Le due tecnologie sono complementari ed il loro simultaneo impiego si giustifica in contesti dove sia presente una significativa offerta di servizi.

Le tecnologie VPN, prestazioni opzionali, si rendono necessarie quando si ritenga che il traffico da gestire nei confronti di specifiche controparti debba essere integralmente protetto dalla possibile lettura di terze parti. Uno di questi casi può essere rappresentato per esempio dal desiderio di un'Amministrazione di usufruire di servizi informatici interni (Contabilità, Personale etc.) in modalità ASP (Application Service Provider) su rete Internet.
In questo caso il collegamento con il fornitore di soluzioni ASP deve necessariamente essere configurato come un'estensione virtuale della rete Intranet dell'Amministrazione, il che può essere realizzato solo attivando una funzionalità di VPN sul Firewall, di concerto con il fornitore di servizi ASP.
Lo standard di riferimento per le VPN è l'IPSEC (RFC2401).

Poiché la tematica della sicurezza concerne non solo la gestione di specifici sistemi di protezione, come quelli menzionati, ma anche la corretta attuazione di politiche di sicurezza sui sistemi che erogano i servizi, è responsabilità del FSR attuare tutte le politiche prescritte (Firewall/Proxy, IDS e VPN) su tutti i sistemi che ospitano i servizi da lui direttamente gestiti presso il proprio Centro Servizi e descritti nel presente capitolo.

3.2.6 Posta Elettronica

Consiste nella gestione di uno o più server di Posta Elettronica dove vengono definite le caselle postali del personale dell'Amministrazione accessibili sia da RUPAR che dall'esterno.

Il livello base di erogazione del servizio prevede l'allocazione presso il Centro Servizi del FSR degli elaboratori che gestiscono la posta elettronica. L'allocazione di almeno uno degli elaboratori presso la PdR è servizio opzionale, che può essere richiesto dall'Amministrazione.

Il servizio osserverà alcuni principi generali:

1. lo scambio di messaggi fra Amministrazioni RUPAR avverrà attraverso sessioni SMTP e/o ESMTP/(S)MIME prioritariamente utilizzando l'infrastruttura RUPAR;
2. ogni utente avrà un solo indirizzo di email, sia per l'infrastruttura RUPAR che per Internet ed indipendentemente dallo standard di formato utilizzato;
3. per supportare lo standard OSI X.400 devono essere attrezzati opportuni mail gateway tra lo standard X.400 e lo standard TCP/IP, referenziato come standard RFC822;

4. i server di posta elettronica dovranno prevedere piena integrazione verso server LDAP (Directory server) e verso l'infrastruttura PKI non appena disponibili;
5. filtraggio di tutti i messaggi ed allegati in ingresso ed in uscita per intercettare messaggi contenti virus, macro-virus, *Trojan Horse* etc., il mittente e/o il destinatario del messaggio devono essere informati via Email dell'avvenuto filtraggio;
6. le sessioni di invio della posta devono prevedere obbligatoriamente la verifica dell'account di posta dell'utente e la sua coincidenza con l'indirizzo mittente della mail (invio controllato mediante autenticazione);
7. le sessioni di invio e ricezione della posta devono prevedere almeno la crittografia della password di autenticazione.

L'accesso al servizio sarà possibile da qualunque host RUPAR mediante uno qualsiasi di questi tipi di connessione:

1. sessioni client/server tipo POP3/IMAP;
2. sessioni HTTP.

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC821, RFC1341, RFC1869, RFC1495, RFC2045, RFC1006, RFC2126, RFC2156 e loro aggiornamenti.

3.2.7 Accesso a WWW

Il servizio consente a tutti gli host della Intranet dell'Amministrazione di ottenere informazioni ospitate su World Wide Web server remoti mediante il protocollo HTTP (HyperText Transfer Protocol).

Il livello base di erogazione del servizio prevede l'allocazione del server proxy/cache presso la PdR.

Il server proxy/cache dovrà gestire:

- proxying e caching di almeno HTTP ed FTP;
- proxying per sessioni sicurizzate SSL;
- trasparent caching;
- autenticazione utente;
- "access control list" intese come liste/filtri per l'accesso al servizio;
- SNMP;
- controllo antivirus dei files scaricati, con avviso in caso di rilevazione di contenuto infetto;
- caching di risoluzioni DNS.

Il supporto del proxy di sessioni di tipo RTP (audio-video *streaming*) è servizio di tipo opzionale, che può essere richiesto dall'Amministrazione e deve essere supportato dal Fornitore; parimenti è possibile che l'Amministrazione richieda il supporto proxy di altri protocolli, in tal caso il Fornitore è libero di supportarli o meno.

Il servizio, amministrato dal FSR, osserverà alcuni principi generali:

1. l'Amministrazione produrrà la lista degli utenti (*username* e *password*) e/o delle postazioni di lavoro abilitate al servizio: la modalità di abilitazione degli utenti al servizio potrà essere basata su una qualsiasi combinazione di queste due informazioni (nome utente e indirizzo IP della stazione utente) a esclusiva discrezione dell'Amministrazione e senza generare differenze di costo del servizio; qualora si utilizzi un'autenticazione basata su password, essa deve essere crittografata mediante protocollo SSL a 128 bit;
2. ad ogni utente verrà attribuita una soglia di impiego della banda;
3. il FSR configurerà e gestirà opportune "black-list" contenenti siti da contenuti potenzialmente dannosi, violenti e/o moralmente indicibili;
4. il FSR dovrà fornire indicazioni su come configurare il servizio sui client del dominio dell'Amministrazione e dovrà garantire anche la configurazione automatica del browser di navigazione fornendo opportuna URL;
5. filtraggio in tempo reale delle sessioni WWW al fine di garantire l'arresto di flussi informativi contenenti minacce di cui si riconosca la "firma" (Virus, Applet Java, Trojan Horse, etc.).

La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC1945 e successivi aggiornamenti.

3.2.8 Trasferimento file

Il servizio consente a tutti gli host della RUPAR di scambiare file di dati, anche di grandi dimensioni, con sistemi remoti mediante il protocollo FTP (File Transfer Protocol). Dalla Intranet dell'Amministrazione l'accesso è

garantito alle postazioni abilitate attraverso il server proxy descritto precedentemente mentre l'elenco delle postazioni da abilitare sarà fornito dall'Amministrazione.

Il livello base di erogazione del servizio prevede l'allocazione del server proxy/cache presso la PdR.

Il servizio potrà essere utilizzato in modalità interattiva oppure essere integrato in altro servizio applicativo e sarà fruibile garantendo sempre le massime condizioni di sicurezza.
Salvo impedimenti oggettivi e/o ad eccezione di accessi a pubblici archivi, eventuali server FTP predisposti su reti RUPAR (DMZ o RSR) dovranno richiedere la cifratura della password durante l'autenticazione dell'utente (supporto AUTH command).
La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC959 e suoi aggiornamenti.

3.2.9 Terminale virtuale

Il servizio consente a tutti gli host abilitati della RUPAR di effettuare sessioni di emulazione terminale con sistemi remoti mediante il protocollo TELNET e/o di Remote Shell. Dalla Intranet dell'Amministrazione l'accesso è garantito alle postazioni abilitate attraverso il server proxy descritto precedentemente mentre l'elenco delle postazioni da abilitare verrà fornito dall'Amministrazione.

Il livello base di erogazione del servizio **non** prevede che esso sia erogato e quindi il servizio è integralmente un servizio opzionale che può essere richiesto dall'Amministrazione e che il Fornitore è tenuto ad erogare; uin questo caso il servizio è erogato per mezzo del server proxy/cache allocato presso la PdR.

Il servizio sarà fruibile garantendo sempre le massime condizioni di sicurezza (SSH, Kerberos).
La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC854 e suoi aggiornamenti/estensioni.

3.2.10 Accesso a news

Il servizio consente a tutti gli host abilitati della RUPAR di partecipare al circuito di distribuzione dei bollettini di informazione (news) mediante il protocollo NNTP (Network News Transfer Protocol).

Il livello base di erogazione del servizio prevede l'allocazione presso il Centro Servizi del FSR degli elaboratori che gestiscono l'archivio delle news.
L'allocazione di almeno uno degli elaboratori presso la PdR è servizio opzionale, che può essere richiesto dall'Amministrazione.

Dalla Intranet dell'Amministrazione l'accesso è garantito alle postazioni abilitate attraverso il server proxy descritto precedentemente mentre l'elenco delle postazioni da abilitare verrà fornito dall'Amministrazione.
La documentazione ufficiale (standard IETF) di riferimento è la seguente: RFC977 e successivi aggiornamenti/estensioni.

3.3 Definizione dei servizi e dei parametri per l'offerta economica

Nella risposta al Bando deve essere offerto il Servizio di Interoperabilità per tutte le seguenti classi dimensionali espresse in termini di Postazioni di Lavoro (PdL) presso la generica Amministrazione:

Servizio di Interoperabilità	
Num. PdL	**Costo per PdL**
Amministrazione	*€/Anno*
n < 25	$I_{<25}$
25 < n < 50	$I_{<50}$
50 < n < 100	$I_{<100}$
100 < n < 250	$I_{<250}$
250 < n < 500	$I_{<500}$
500 < n < 1000	$I_{<1000}$
n > 1000	$I_{>1000}$

Tabella 2 - Classi di servizio per interoperabilità RUPAR

Per ognuna delle classi di servizio di Tabella 2 dovranno essere indicati il costo per l'erogazione dei servizi di interoperabilità e le modalità operative gestionali del livello base di erogazione.

Ognuno di essi dovrà essere un costo:

- omnicomprensivo relativo al livello base per ognuno dei servizi previsti nel presente Capitolato, ivi inclusi i Servizi di Supporto successivamente specificati e all'utilizzo di tutte le apparecchiature neces-

sarie (server, infrastrutture, etc.) per fornire il servizio alle Amministrazioni;

- di tipo "flat" (canone annuo), indipendente sia dal tempo in cui l'Amministrazione trasmette o riceve traffico sia dal volume del traffico stesso;
- privo di voci una-tantum (p. es. attivazione).

Nella risposta al Bando devono essere, altresì, offerti tutti i seguenti servizi aggiuntivi che il FSR deve rende disponibili come opzioni:

1. Servizio di Gestione dei Nomi (DNS)
   - allocazione di un server presso la PdR
2. Servizio di Directory
   - allocazione di un server presso la PdR
3. Servizio di Sicurezza
   - attivazione e gestione della DMZ presso la PdR
   - attivazione e gestione della RSR presso la PdR
   - gestione di un elaboratore su DMZ e/o RSR: il costo comprende, oltre all'attivazione delle prescritte azioni sul Firewall, anche prestazioni opzionali relative al Servizio di Trasporto (indirizzamento) al Servizio di Gestione Nomi (nome canonico dell'elaboratore ed eventuali nomi alias di host virtuali)
   - attivazione e gestione in modo selettivo del servizio NAT/PAT per le stazioni dell'Intranet
   - attivazione e gestione IDS sulla PdR
   - attivazione e gestione funzionalità VPN sulla PdR
   - gestione di una VPN su richiesta dell'Amministrazione: il costo comprende, oltre all'attivazione delle prescritte azioni sul

Firewall, anche prestazioni opzionali relative al Servizio di Trasporto (indirizzamento) al Servizio di Gestione Nomi

4. Servizio di Posta Elettronica
   - allocazione di un server presso la PdR
5. Servizio News
   - allocazione di un server presso la PdR
6. Servizio di accesso a WWW
   - supporto proxy audio-video streaming via RTP
7. Servizio di Terminale Virtuale
   - supporto del servizio

Tutti i servizi opzionali possono essere richiesti dall'Amministrazione ed il Fornitore è tenuto ad erogarli osservando le prescrizioni tecniche minime del presente Capitolato Tecnico, i costi dei servizi opzionali sono interamente a carico delle Amministrazioni e non sono oggetto di finanziamento né da parte della Regione Puglia né da parte del Fornitore.

3.4 La Qualità tecnica del servizio

La qualità tecnica del singolo servizio di interoperabilità si misura mediante le seguenti metriche:

1. disponibilità temporale
2. prestazioni di erogazione

La disponibilità del servizio è misurata in base ai due parametri di Uptime (Tempo ininterrotto di disponibilità di un servizio) e MTBF (Mean Time Between Failures, tempo che intercorre tra due guasti consecutivi dello stesso servizio).

La disponibilità di base richiesta è di 24 ore al giorno e 365 giorni l'anno.

I valori previsti sono i seguenti:

1. Uptime > 99,5%
2. MTBF > 2000 ore

Si noti che il parametro di Uptime è comprensivo anche degli interventi con caratteristiche bloccanti del servizio, programmati per finalità di manutenzione preventiva e/o evolutiva.

Per tutti i servizi si richiede che eventuali interruzioni di servizio per manutenzioni siano comunicate con un anticipo di almeno **3 giorni**.

Per le prestazioni di erogazione dei singoli servizi intendiamo la velocità con cui servizi interattivi o batch vengono fruiti dagli utenti in condizioni di rete normali.

Nel caso di servizi interattivi e relativamente alle prestazioni standard di trasferimento dati end-to-end del livello di trasporto in condizioni normali, le prestazioni dei servizi di interoperabilità potranno prevedere un ulteriore delay non superiore al 5% rispetto alle prestazioni ottenibili senza l'impiego del/i servizio/i di interoperabilità.

Per servizi batch, tipo le sessioni SMTP tra Mail Transfer Agent, le prestazioni complessive devono prevedere, oltre al delay definito in precedenza, anche una soglia di messaggi presenti nella outgoing spool directory dell'MTA; il numero di messaggi massimo nella coda di spool di un MTA non deve superare le dieci unità (sono esclusi i messaggi etichettati "deferred" a causa di indisponibilità del server SMTP di destinazione).

4 La Sicurezza

Il Fornitore è responsabile della sicurezza sia fisica che logica del servizio ed a tal fine dovrà predisporre, attuare ed aggiornare costantemente una politica della sicurezza, sia fisica che logica, conforme alle prescrizioni emanate dal Centro Tecnico. Nel Documento Programmatico della sicurezza e nelle specifiche tecniche di dettaglio della sicurezza consegnate al momento dell'attivazione del servizio il Fornitore dovrà prevedere specifiche procedure atte a regolare la gestione della sicurezza almeno per le seguenti aree:

- analisi dei rischi,
- amministrazione della sicurezza,
- audit,
- test ciclici di impenetrabilità,
- incidenti di sicurezza,
- allarmi e interventi,
- controllo e analisi delle registrazioni relative alla sicurezza.

Il Fornitore, nell'ambito della propria organizzazione, condurrà le operazioni in maniera da:

- minimizzare la probabilità di intercettazione, accesso, modifiche, distruzione non autorizzate o l'uso improprio relativamente alle informazioni degli utenti in transito nella RUPAR per la parte di propria competenza;
- minimizzare la probabilità di accesso, comunicazione, modifiche, distruzione non autorizzate o uso improprio delle informazioni delle Amministrazioni comunque residenti negli apparati da esso gestiti.

Il Centro Tecnico può adeguare le prescrizioni minime di sicurezza contenute nel presente Capitolato:

- al verificarsi di variazioni del livello di rischio cui sono soggetti i servizi o i dati delle Amministrazioni
- a seguito di modifiche della tecnologia informatica utilizzata per erogare i servizi
- in caso di disponibilità di tecnologie più evolute nell'ambito della sicurezza.

Il Fornitore è tenuto a mantenere aggiornato il sistema di sicurezza rispetto a tali revisioni.

4.1 Organizzazione della Sicurezza

Il Fornitore deve definire una struttura dedicata alla sicurezza.
Le apparecchiature di comunicazione, informatiche, i sistemi, i software di base ed applicativi gestiti devono avere un "Amministratore" esplicitamente individuato. Le procedure organizzative osservate dal personale del Fornitore devono essere formalizzate in specifici documenti, da tenere costantemente aggiornati: il personale del Fornitore deve essere opportunamente sensibilizzato sui rischi di sicurezza inerenti alla RUPAR e addestrato sull'uso delle misure di protezione.

4.2 Gestione della Sicurezza

Il Fornitore nel Documento Programmatico di gestione della sicurezza, allegato alla Documentazione Tecnica del progetto dovrà prevedere specifiche procedure atte a regolare la gestione della sicurezza per le aree di seguito specificate.

Analisi dei rischi. Il Fornitore deve condurre l'analisi dei rischi su base sistematica, con cadenza almeno annuale. Tale analisi va ripetuta a seguito di attacchi o incidenti gravi di sicurezza o per variazioni significative dell'architettura della RUPAR. Le metodologie di conduzione dell'analisi dei rischi saranno concordate con il Centro Tecnico.

Amministrazione della sicurezza. Il Fornitore deve definire le regole ed i processi per l'Amministrazione della sicurezza rispetto alle proprie strutture organizzative e rispetto ai rapporti con le Amministrazioni, gli altri FSR ed il Centro Tecnico. In particolare devono essere indicati i criteri con cui sono assegnati all'interno del Centro di Gestione gli accessi alle componenti hardware e software impiegate per erogare i Servizi e le relative autorizzazioni. Nel Documento Programmatico deve essere previsto un processo periodico di revisione delle utenze e delle autorizzazioni di sicurezza così come deve essere prevista l'immediata cancellazione delle utenze relative al personale che risolve il rapporto di lavoro col Fornitore o non più operativo presso la struttura di erogazione dei servizi RUPAR.
Ogni *user-id* relativa al personale operativo deve poter essere riconducibile ad un singolo individuo ed essere coerente con le effettive necessità di lavoro.
Il Fornitore deve permettere al Centro Tecnico di verificare, su richiesta, lo stato delle utenze e gli archivi con le registrazioni ed i parametri di sicurezza.

Audit. Su base periodica (annuale) il sistema di sicurezza deve essere oggetto di un approfondito audit. L'audit deve essere condotto da una primaria società specializzata scelta dal Fornitore, da esso distinta, previo gradimento del Centro Tecnico e che opererà sotto la vigilanza del Centro Tecnico e delle Amministrazioni, ciascuno per quanto di propria competenza. I risultati dell'audit e gli eventuali piani di rientro devono essere comunicati al Centro Tecnico ed alle Amministrazioni interessate. Il Centro Tecnico e le Amministrazioni potranno, ciascuno per quanto di competenza e con un preavviso di tre settimane, effettuare ulteriori attività di audit secondo modalità che saranno concordate con il Fornitore.

Test ciclici di impenetrabilità. Il Fornitore deve effettuare ogni anno un test di impenetrabilità sugli apparati e sui servizi supportati. I testi di impenetrabilità devono essere condotti da una primaria società specializzata scelta dal Fornitore, da esso distinta, previo gradimento del Centro Tecnico e che opererà sotto la vigilanza del Centro Tecnico e delle Amministrazioni, ciascuno per quanto di propria competenza. Scopo dei test è quello di verificare, senza arrecare danno ai dati ed ai servizi, l'efficacia delle misure di sicurezza adottate dal Fornitore. Devono essere usati tool, specializzati e allo stato dell'arte, per individuare le debolezze della rete, dei sistemi e dei servizi. Dopo ogni test deve essere prodotto il report dei risultati che deve essere fornito alle Amministrazioni ed al Centro Tecnico per le parti di rispettiva competenza; devono inoltre essere messe in atto le opportune azioni correttive, se rivelatesi necessarie.

Test discrezionali di impenetrabilità. Il Centro Tecnico potrà effettuare autonomamente test di impenetrabilità. I test effettuati dal Centro Tecnico, per il Dominio della Rete unitaria, saranno di due tipologie:

a) dall'esterno della RUPAR;

b) dall'interno della RUPAR.

I test potranno essere condotti senza preavviso con frequenza e durata a discrezione del Centro Tecnico che informerà il Responsabile della sicurezza del Fornitore all'inizio ed al termine di ogni test.

Nel caso i test mettano in evidenza delle carenze rispetto alle specifiche tecniche di sicurezza, la situazione deve essere corretta come previsto nel Contratti di servizio di cui agli Allegati A e B.

Verifiche d'architettura. Il Fornitore deve attivare un processo che effettui controlli, possibilmente automatici, per verificare che gli elementi chiave ai fini della sicurezza siano integri.

Incidenti di sicurezza. Le violazioni delle prescrizioni di sicurezza e gli eventi negativi connessi con lo stato della sicurezza delle informazioni (quali ad esempio: intercettazione, integrità, riservatezza, disponibilità) devono essere oggetto di raccolta, analisi e piani di intervento.

Allarmi e interventi. Il Fornitore dovrà indicare nel Documento Programmatico di gestione della sicurezza, le componenti hardware e software considerate critiche per la sicurezza dei Servizi erogati. Tali componenti devono essere dotate di adeguati sistemi di allarme. Le segnalazioni devono essere concentrate in modo che sia possibile rapidamente valutare la gravità della situazione e far partire le opportune azioni difensive. Il Responsabile della Sicurezza deve poter disporre della capacità di un pronto intervento.

Controllo e analisi dei log. Al fine di individuare comportamenti scorretti o intrusioni è fondamentale disporre di adeguati processi e strumenti automa-

tici di controllo dei log. Il Documento Programmatico di gestione della sicurezza dovrà dettagliare i log gestiti, per quanto tempo sono mantenuti e le misure specifiche di protezione. Deve essere data la possibilità al Centro Tecnico ed alle Amministrazioni, a ciascuno per quanto di propria competenza, di accedere ed analizzare i log in questione.

Norme per il personale che opera nel Centro di Gestione. L'accesso ai dati delle Amministrazioni, normalmente proibito, può avvenire da parte del personale operativo nella gestione solo se esplicitamente richiesto dall'Amministrazione. L'uso delle apparecchiature facenti parte della RUPAR è permesso solo per svolgere le attività previste per l'esecuzione del servizio

5 I servizi di supporto

Sono previsti i seguenti servizi:

- *Help Desk*, finalizzato al supporto dell'utenza finale a fronte di problemi o necessità di aiuto
- *Monitoraggio*, finalizzato alla sorveglianza dei servizi erogati, al fine di poter intervenire in modo tempestivo al manifestarsi dei problemi, prima che a darne notizia sia l'utente finale
- *Gestione Dati*, finalizzato alla salvaguardia dei dati delle Amministrazioni utenti.
- *Registrazione attività ed eventi*, finalizzato alla raccolta e all'archiviazione delle informazioni relative all'attività svolta sulla rete da parte dell'utenza

5.1 Help Desk

E' erogato attraverso la disponibilità dei seguenti strumenti di interazione resi disponibili all'utenza finale:

- un numero verde telefonico
- un indirizzo di posta elettronica
- una applicazione Web

Tutti i canali di interazione devono essere presidiati e devono essere gestiti dagli operatori in modo coerente con un'unica procedura di gestione delle richieste che permetta la loro elaborazione, tenendo traccia della chiamata e di alcuni attributi ad essa relativi quali: autore della richiesta, motivo della richiesta, tempo di risoluzione del problema etc.

Il formato esatto dell'archivio delle chiamate che dovrà essere così realizzato da ogni fornitore, sarà specificato dal CT, in modo che sia possibile far con-

vergere questi dati in un'unica banca dati del CT.
Oltre che gli interventi richiesti dall'utente, dovranno essere gestiti dalla stessa procedura anche gli allarmi generati dal servizio di supporto di "Monitoraggio", come di seguito specificato.

Quello descritto è uno dei due flussi operativi che intercorrono tra i due servizi, il secondo flusso è rappresentato dal possibile supporto che il servizio di Monitoraggio può fornire al servizio di Help Desk in un'analisi in tempo reale dei problemi segnalati dall'utente.

Agli utenti che attivano una segnalazione di un problema deve essere rilasciato un identificativo della segnalazione (*trouble ticket*) che gli consenta di tracciare l'evoluzione della soluzione del problema accedendo nuovamente al servizio stesso.

Per quanto concerne la gestione di questa tipologia di accessi, la banca dati della procedura di Help Desk deve essere accessibile in rete RUPAR per mezzo di un browser WWW.
Inoltre, poichè alcuni malfunzionamenti possono concernere proprio l'accesso alla rete, lo stesso servizio deve essere disponibile anche per via telefonica.

Le informazioni della procedura di Help Desk saranno oggetto di trasferimento verso il CT (Servizio di Registrazione attività ed eventi) per consentire elaborazioni statistiche della qualità di servizio complessiva della RUPAR.

5.2 Monitoraggio della rete e dei sistemi

E' erogato per mezzo di operatori che sorvegliano l'andamento dei servizi

intervenendo in tempo reale a risolvere problemi che eventualmente vengano segnalati dai sistemi di gestione e/o dall'Help Desk.

Parimenti gli operatori del Servizio di Monitoraggio accedono al Servizio di Help Desk per aprire, a fini rendicontativi, incidenti rilevati per mezzo dei sistemi di gestione.

Il servizio deve disporre di due canali di accesso (telefonico e posta elettronica), ignoti all'utenza e riservati all'interazione con gli analoghi servizi degli altri Fornitori e con il CT.

5.3 Gestione Dati

E' erogato per mezzo di procedure e strumentazioni idonee a realizzare copie di salvataggio dei dati dell'Amministrazione che garantiscano che i dati non vadano persi a fronte di guasti hardware delle apparecchiature che gestiscono il servizio.

In questo contesto si intende per servizio un servizio di interoperabilità, dato che le problematiche che concernono i servizi applicativi, pur essendo simili, sono di competenza dei relativi fornitori.

Si distingue tra il guasto di una singola componente (p. es. disco), a fronte del quale l'integrità dei dati deve essere sempre totale, e il disastro (p. es. incendio) che distrugga l'intero complesso di attrezzature per mezzo delle quali un servizio viene erogato per la specifica Amministrazione.

Per questo secondo caso (problematica di *Disaster Recovery*), si definiscono i seguenti tre livelli di servizio:

- Alta criticità: si richiede che l'integrità dei dati sia garantita totalmente (schema di duplicazione dei dati in *Real Time* o in *Near Real Time*, con remotizzazione fisica dei due siti di allocazione dei dati)
- Media criticità: si accetta la perdita di dati fino ad un tempo massimo di un giorno (schema di backup giornaliero dei dati, con remotizzazione fisica del sito di allocazione del backup rispetto a quello di esercizio)
- Bassa criticità: si accetta la perdita di dati fino ad un tempo massimo di una settimana (schema di backup settimanale dei dati, con remotizzazione fisica del sito di allocazione del backup rispetto a quello di esercizio)
- Minima criticità: si accetta la salvaguardia delle informazioni relative a specifici momenti della gestione del servizio: p. es. attivazione, importanti variazioni di configurazione (schema di backup aperiodico dei dati, con remotizzazione fisica del sito di allocazione del backup rispetto a quello di esercizio)

Per i servizi erogati presso il Centro Servizi del FSR è richiesto un livello di garanzia rispetto al Disaster Recovery almeno di criticità media. I servizi a livello base erogati presso la PdR, poiché non contengono informazioni pertinenti l'Amministrazione oltre a quelle specifiche di configurazione degli apparati della PdR, non necessitano di un livello superiore a quello di minima criticità. Livelli superiori possono essere richiesti dalle Amministrazioni contestualmente all'attivazione di livelli di servizio opzionali.

5.4 Registrazione Attività ed Eventi

Il Servizio ha il compito di archiviare e trasferire verso il CT il log delle atti-

vità e degli eventi dei principali servizi di interoperabilità: Posta Elettronica, Accesso a WWW e Sicurezza (funzione Firewall intesa come report sui servizi applicativi acceduti a livello di Centro Servizi, o anche a livello di reti RSR e DMZ (se presenti) ed anche report del servizio NAT/PAT se attivato su richiesta dell'Amministrazione), nonché del servizio di supporto Help Desk.

Il formato di ogni singolo record di registrazione e le modalità di trasferimento (temporizzazione, protocolli etc.) saranno specificati dal CT al momento della attivazione esecutiva della rete. In ogni caso tutti record del log dovranno contenere un riferimento temporale derivato direttamente dal servizio di Tempo Ufficiale di Rete e non saranno specificate in dettaglio informazioni relative alle singole stazioni utente, ma piuttosto un'informazione globale indicante l'Amministrazione a cui il log si riferisce.

Per quanto concerne il Servizio di Trasporto non è previsto che si avvalga di questo servizio di supporto, dato che le informazioni relative alla attività e agli eventi saranno gestiste direttamente dal CT mediante il proprio servizio di Gestione Sistemi e Rete via SNMP.

Lo scopo della costituzione presso il CT di una banca dati complessiva dell'utilizzazione dei servizi sulla RUPAR ha eminentemente scopi statistici e di pianificazione, consentendo uno studio di monitoraggio approfondito nel tempo dell'utilizzo degli stessi da parte delle Amministrazioni utente.

Ogni responsabilità riguardo alla riservatezza dei dati comunicati al CT da parte del Fornitore rimane in capo al CT esattamente come in capo al Fornitore ognuno per la parte di propria competenza.

6 Documentazione tecnica di progetto

Deve essere presentata una relazione tecnica che descriva l'architettura della rete che si intende realizzare.

Per quanto concerne il Servizio di Trasporto devono essere dettagliate le scelte a livello di:

- collegamenti geografici tra i nodi della rete;
- nodi di rete e protocolli di trasporto;
- piattaforme hardware e software previste;
- collegamenti agli EPO-LP;
- modalità di raccolta dell'utenza;
- gestione delle BMG.

Per quanto concerne il Servizio di Interoperabilità di Base devono essere dettagliate le scelte a livello di:

- soluzioni tecniche di dettaglio, in termini di piattaforme hardware e software e delle loro interconnessioni, per ognuno dei servizi di Interoperabilità;
- specifiche tecniche di dettaglio delle misure di sicurezza;
- modalità di raccolta dell'utenza;
- piattaforme hardware e software previste.

Infine il progetto deve specificare:

- organizzazione e piattaforma tecnologica del Centro di Gestione;
- organizzazione e infrastruttura tecnologica dei Servizi di Supporto;
- Documento Programmatico di gestione della sicurezza.

Tecnopolis CSATA

Regione Puglia

Rete Unitaria della Pubblica Amministrazione Regionale

(R.U.P.A.R)

Capitolato Tecnico del Servizio di Firma Digitale

(prodotto nell'ambito della Convenzione approvata dalla Giunta Regionale con deliberazione n. 1162 del 10/8/2001)

Allegato D

Versione 2.1 del 5/8/2002

INDICE

1 Introduzione

Gli scopi, le modalità realizzative, le modalità di finanziamento e le specificazioni tecniche relative alla costituenda RUPAR sono contenute nel documento “Piano Strategico di Sviluppo” della RUPAR-Puglia, che costituisce la premessa indispensabile alla comprensione del quadro d’insieme.

Va precisato tuttavia che per qualsiasi discordanza formale o sostanziale si dovesse eventualmente riscontrare tra il documento “Piano Strategico di Sviluppo della RUPAR” ed il presente Capitolato Tecnico, comprensivo dell’Allegato A che ne fa integralmente parte, l’unico riferimento valido ai fini dell’espletamento della gara di selezione è quanto contenuto nel presente Bando.

Il Fornitore di Servizi di Firma Digitale (FSFD) deve fornire il fondamentale servizio di rilascio e gestione dei certificati digitali di firma a valore legale (Certificati a norma AIPA) alle Amministrazioni che dovessero rivolgersi a lui per ottenere il servizio.
Questo è il servizio coperto dal cofinaziamento regionale in ragione del 50% dei costi, eventuali servizi aggiuntivi di rilascio di certificati di altro tipo sono da considerare servizi opzionali liberamente erogati dal Fornitore alle Amministrazioni che ne dovessero fare richiesta, a loro esclusivo e totale carico.

2 Specificazione tecnica del Servizio di Firma Digitale

2.1 Requisiti tecnologici ed organizzativi

Il **Servizio di Firma Digitale** deve essere conforme totalmente alle prescrizioni tecniche dell'AIPA, così come gli standard tecnici pertinenti sono quelli indicati dall'AIPA come vincolanti.

I requisiti specifici da rispettare per poter erogare il servizio nella RUPAR Puglia sono i seguenti:

1. rilascio e gestione dei certificati digitali di firma a valore legale (Certificati a norma AIPA);
2. gestione dell'identificazione delle persone e del supporto fisico di firma (smart card) presso propri uffici dislocati almeno in tutti i capoluoghi di provincia;
3. disponibilità all'erogazione del servizio di verifica dei certificati e delle relative liste di revoca (CRL) anche mediante un collegamento diretto con il Centro Tecnico al fine di supportare tutto il traffico di validazione dei certificati della RUPAR in modo indipendente dalla rete Internet.

Tale collegamento potrà essere attivato dal Centro Tecnico già al momento della partenza della rete RUPAR, potrà essere ad una velocità compresa tra 64 e 2048 Kbps su una tecnologia di rete geografica concordata con il fornitore (CDN, Frame Relay etc.) e sarà realizzato mediante protocollo TCP/IP. La disponibilità del Fornitore dovrà essere comprensiva della strumentazione di rete allocata presso il suo Centro Servizi per terminare il collegamento geografico.

L'indirizzamento di questo collegamento sarà realizzato congiuntamente da Fornitore e Centro Tecnico in base a tutti i vincoli che dovessero essere determinati in fase di attivazione.

2.2 Definizione dei servizi e dei parametri per l'offerta economica

L'unica classe di servizio prevista è quella del **certificato** digitale di firma a **valore legale** (Certificato a norma AIPA).

Per questo servizio deve essere indicato il costo annuo:

- **omnicomprensivo**, ivi inclusi: la *smart card* che ospita il certificato, il lettore di smart card in ragione di un lettore ogni cinque certificati di firma, il servizio di marca temporale, nella misura di almeno n.10 *timestamp* per ogni certificato di firma, utilizzabile eventualmente in maniera cumulativa dall'Amministrazione , tutti i servizi di supporto richiesti nel presente capitolato tecnico, il supporto presso i propri uffici e presso i punti di accesso al servizio a livello provinciale.
- di tipo "***flat***" (canone annuo), indipendente dal numero di utilizzi del certificato effettuato dall'Amministrazione
- **privo di voci una-tantum** (p. es. attivazione)

2.3 La Qualità tecnica del servizio

La qualità tecnica del Servizio di trasporto si misura mediante le seguenti metriche:

1. disponibilità del servizio
2. tempo di risposta dei servizi

La disponibilità di base richiesta è:

1. 24 ore al giorno e 365 giorni l'anno per il servizio di accesso online al Registro dei certificati e alle Liste dei certificati revocati/sospesi; questo servizio deve essere caratterizzato dai seguenti valori di qualità:
    - Uptime > 99,5% (Tempo ininterrotto di disponibilità di un servizio)
    - MTBF > 2000 ore (Mean Time Between Failures, tempo che intercorre tra due guasti consecutivi dello stesso servizio)

    Si noti che il parametro di Uptime è comprensivo anche degli interventi, con caratteristiche bloccanti del servizio, programmati per finalità di manutenzione preventiva e/o evolutiva.

2. Dalle 08:00 alle 18:00 di tutti i giorni feriali escluso il Sabato per i servizi di emissione, rinnovo, sospensione, revoca e riattivazione dei certificati di sottoscrizione e di emissione marche temporali

Per tutti i servizi si richiede che eventuali interruzioni di servizio per manutenzioni siano comunicate con un anticipo di almeno 3 giorni.

Il tempo di risposta dei servizi deve essere nel 95% dei casi nei limiti della seguente tabella:

Parametro da rilevare	**Valore massimo**
Tempo massimo di emissione, rinnovo, riattivazione di un certificato di sottoscrizione	2 gg
Tempo massimo di revoca, sospensione di un certificato di sottoscrizione	10'
Tempo massimo di emissione, consegna di un dispositivo di firma	5 gg
Tempo massimo di blocco di un dispositivo di firma	10'
Tempo massimo di emissione di una marca temporale	20'
Produzione dei report sui livelli di Servizio dalla fine del periodo prescritto	10 gg
Tempo di accesso online al Registro dei certificati e alle Liste dei certificati revocati/sospesi	40”

Il tempo di accesso online al Registro viene misurato in situazioni in cui non vi sia congestione del collegamento tra Centro Servizi del Fornitore e Centro Tecnico, imputabile al Centro Servizi del Fornitore.

Questa situazione è da escludere nel caso di collegamento dedicato; eventuali situazioni di congestione del collegamento diretto dedicato tra Centro Servizi del Fornitore e Centro Tecnico saranno gestite dal Centro Tecnico aumentando la velocità dello stesso.

3 I servizi di supporto

Sono previsti i seguenti servizi:

- *Help Desk*, finalizzato al supporto dell'utenza finale a fronte di problemi o necessità di aiuto
- *Monitoraggio*, finalizzato alla sorveglianza dei servizi erogati, al fine di poter intervenire in modo tempestivo al manifestarsi dei problemi, prima che a darne notizia sia l'utente finale
- *Registrazione attività ed eventi*, finalizzato alla raccolta e all'archiviazione delle informazioni relative all'attività svolta sulla rete da parte dell'utenza

3.1 Help Desk

E' erogato attraverso la disponibilità dei seguenti strumenti di interazione resi disponibili all'utenza finale:

- un numero verde telefonico
- un indirizzo di posta elettronica
- una applicazione Web

Tutti i canali di interazione devono essere presidiati e devono essere gestiti dagli operatori in modo coerente con un'unica procedura di gestione delle richieste che permetta la loro elaborazione, tenendo traccia della chiamata e di alcuni attributi ad essa relativi quali: autore della richiesta, motivo della richiesta, tempo di risoluzione del problema etc.

Il formato esatto dell'archivio delle chiamate che dovrà essere così realizzato da ogni fornitore, sarà specificato dal CT, in modo che sia possibile far convergere questi dati in un'unica banca dati del CT.

Oltre che gli interventi richiesti dall'utente, dovranno essere gestiti dalla stessa procedura anche gli allarmi generati dal servizio di supporto di "Monitoraggio", come di seguito specificato.

Quello descritto è uno dei due flussi operativi che intercorrono tra i due servizi, il secondo flusso è rappresentato dal possibile supporto che il servizio di Monitoraggio può fornire al servizio di Help Desk in un'analisi in tempo reale dei problemi segnalati dall'utente.

Agli utenti che attivano una segnalazione di un problema deve essere rilasciato un identificativo della segnalazione (***trouble ticket***) che gli consenta di tracciare l'evoluzione della soluzione del problema accedendo nuovamente al servizio stesso.

Per quanto concerne la gestione di questa tipologia di accessi, la banca dati della procedura di Help Desk deve essere accessibile in rete RUPAR per mezzo di un browser WWW.

Le informazioni della procedura di Help Desk saranno oggetto di trasferimento verso il CT (Servizio di Registrazione attività ed eventi) per consentire elaborazioni statistiche della qualità di servizio complessiva della RUPAR.

3.2 Monitoraggio della rete e dei sistemi

E' erogato per mezzo di operatori che sorvegliano l'andamento dei servizi intervenendo in tempo reale a risolvere problemi che eventualmente vengano segnalati dai sistemi di gestione e/o dall'Help Desk.

Parimenti gli operatori del Servizio di Monitoraggio accedono al Servizio di Help Desk per aprire, a fini rendicontativi, incidenti rilevati per mezzo dei sistemi di gestione.

Il servizio deve disporre di due canali di accesso (telefonico e posta elettronica), ignoti all'utenza e riservati all'interazione con gli analoghi servizi degli altri Fornitori della RUPAR e con il Centro Tecnico.

3.3 Registrazione Attività ed Eventi

Il Servizio ha il compito di archiviare e trasferire verso il CT il log delle attività e degli eventi del servizio (verifica certificati e CRL), nonché del servizio di supporto Help Desk.

Il formato di ogni singolo record di registrazione e le modalità di trasferimento (temporizzazione, protocolli etc.) saranno specificati dal CT al momento della attivazione esecutiva della rete.

Lo scopo della costituzione presso il CT di una banca dati complessiva dell'utilizzazione dei servizi sulla RUPAR ha eminentemente scopi statistici e di pianificazione, consentendo uno studio di monitoraggio approfondito nel tempo dell'utilizzo degli stessi da parte dell'utente finale.

Ogni responsabilità riguardo alla riservatezza dei dati comunicati al CT da parte del Fornitore rimane in capo al CT esattamente come in capo al Fornitore ognuno per la parte di propria competenza.

4 Documentazione tecnica di progetto

Deve essere presentata una relazione tecnica che descriva l'architettura del Servizio che si intende realizzare.

Esso deve comprendere:

- descrizione delle piattaforme hardware/software utilizzate sia nel Centro Servizi che presso l'utente (smart card, lettori etc.)
- descrizione dei tools che l'utenza può o deve utilizzare per accedere al servizio
- dimostrazione dell'avvenuta adozione di tutte le vigenti prescrizioni dell'AIPA e del Centro Tecnico della RUPA nazionale per quanto concerne l'interoperabilità con le altre Autorità di Certificazione
- descrizione della/e tipologia/e preferita/e per il collegamento dedicato con il Centro Tecnico
- modalità di raccolta e gestione dell'utenza

Infine il progetto deve specificare:

- organizzazione e infrastruttura tecnologica dei Servizi di Supporto
- Documento Programmatico di gestione della sicurezza

Tecnopolis CSATA

Regione Puglia

Rete Unitaria della Pubblica Amministrazione Regionale

(R.U.P.A.R)

Capitolato Tecnico del Servizio di locazione dei nodi (EPO-LP) della RUPAR

(prodotto nell'ambito della Convenzione approvata dalla Giunta Regionale con deliberazione n. 1162 del 10/8/2001)

Allegato E

Versione 2.1 del 5/8/2002

INDICE

1 Introduzione

Gli scopi, le modalità realizzative, le modalità di finanziamento e le specificazioni tecniche relative alla costituenda RUPAR sono contenute nel documento "***Piano Strategico di Sviluppo***" della RUPAR-Puglia, che costituisce la premessa indispensabile alla comprensione del quadro d'insieme.

Va precisato tuttavia che per qualsiasi discordanza formale o sostanziale si dovesse eventualmente riscontrare tra il documento "Piano Strategico di Sviluppo della RUPAR" ed il presente Capitolato Tecnico, comprensivo dell'Allegato B al bando che ne fa integralmente parte, l'unico riferimento valido ai fini dell'espletamento della gara di selezione è quanto contenuto nel presente Bando.

Il **Fornitore del Servizio di Locazione degli EPO-LP** (FSL-EPO) deve fornire il servizio di ospitalità degli Armadi che costituiscono gli EPO-LP della RUPAR Puglia.

Questo è il servizio coperto dal cofinaziamento regionale in ragione del 50% dei costi, mentre il rimanente 50% deve essere coperto dal Fornitore aggiudicatario.

2 Specificazione tecnica del Servizio di Locazione degli EPO-LP

2.1 Requisiti tecnologici ed organizzativi

Il servizio richiesto consiste in n. 4 Siti, ubicati nelle città di Foggia, Taranto, Brindisi e Lecce, in cui il Fornitore accetta di alloggiare gli Armadi degli EPO-LP della RUPAR, che sono gestiti direttamente dal Centro Tecnico.

Un EPO-LP della RUPAR è costituito da un armadio avente i seguenti dati tecnici:

- dimensioni LxPxH = 600x600x2200mm
- accessibilità anteriore e posteriore
- assorbimento elettrico fino a 2 Kw (tensione di 220Vac)

E' necessario prevedere per l'armadio una sufficiente area operativa per consentire l'operatività anteriore e posteriore.

L'alimentazione elettrica deve avere carattere di stabilità di tensione entro 1% della tensione nominale e continuità garantita di almeno 4 ore anche nel caso di interruzione della rete elettrica.

Il Sito deve essere dotato di rilevatori di incendio ed adeguati impianti di sicurezza.

Il Sito deve essere dotato di facility di accesso per il trasporto di apparati all'interno, in particolare, se non ubicato al piano terra, deve disporre di adeguati elevatori/montacarichi utilizzabili a questo scopo.

L'ambiente deve essere condizionato in modo da garantire una temperatura di esercizio tra 20°C e 25 °C ed adeguato livello di umidità.

Negli Armadi dovranno essere allocate, a cura e sotto il controllo del Centro Tecnico, apparecchiature dei Fornitori del Servizio RUPAR (FSR) e precisamente un router per ognuno di essi.
Inoltre il Centro Tecnico ed ogni FSR dovranno terminare negli Armadi dei circuiti geografici di Telecomunicazioni, che quindi dovranno poter essere portati all'interno del Sito per poter installare i relativi DCE negli Armadi del EPO-LP.

I circuiti di cui sopra potranno essere forniti da Fornitori distinti dal FSL-EPO, ciò non di meno il FSL-EPO dovrà accettare la loro terminazione all'interno del Sito negli armadi del EPO-LP.

Il Sito dovrà essere ubicato nella cerchia urbana della città.

Gli Armadi degli EPO-LP saranno chiusi e dotati di meccanismi di apertura a chiave che sarà in possesso solo del personale abilitato, il FSL-EPO dovrà garantire il più possibile la protezione degli stessi da tentativi di effrazione e/o danneggiamento.

L'accesso al Sito dovrà essere ristretto e consentito solo a personale identificato del FSL-EPO, del Centro Tecnico e degli FSR selezionati per la RUPAR.

Il FSL-EPO dovrà tenere all'uopo un Registro, che gli verrà fornito dal CT, dove annoterà tutti gli interventi di personale dei FSR e/o del CT presso i EPO-LP. Estratti di detto Registro dovranno essere inviati periodicamente al CT, per un controllo della congruenza delle attività.

L'accesso dovrà essere sempre consentito, senza preavviso, nella fascia oraria 09:00 – 17:00 di tutti i giorni feriali; per accessi in orari diversi deve essere prevista una procedura che li renda possibili con un preavviso di 24 ore.

2.2 Parametri per l'offerta economica

Per questo servizio deve essere indicato:

1. il costo di attivazione una-tantum per ognuno dei quattro siti;
2. il costo annuo omnicomprensivo (canone) per tutti e quattro i Siti, incluse tutte le prestazioni richieste: condizionamento, UPS etc.

Il costo presentato dal Fornitore dovrà essere analiticamente documentato con l'indicazione di tutte le voci pertinenti.

Si considerano voci pertinenti quelle ammesse come tali dall'Autorità Garante delle Comunicazioni (AGCOM) per i servizi di housing per interconnessione in centrale ed in particolare le seguenti voci con la specificazione del criterio di calcolo del costo:

- Costo della superficie al metro quadro commerciale
- Servizio di energia (comprensivo di trattamento energia, UPS e gestione amministrativo-contabile) per Kw di assorbimento garantito

- Servizio di condizionamento ad uso condiviso, per Kw di potenza dissipata
- Servizi di Facility Management (Manutenzione impianti tecnologici, impianti elevatori, estintori e servizi di pulizia, smaltimento rifiuti e prestazioni accessorie come disinfestazione/derattizzazione e sgombero neve) per mq commerciale
- Servizi di Security (Vigilanza, Portierato, Gestione allarmi e Abilitazione accessi) per mq commerciale

L'importo di ogni voce potrà essere indicato in proporzione all'effettiva incidenza sul Servizio oggetto del presente Capitolato.

2.3 La Qualità tecnica del servizio

La qualità tecnica del Servizio si misura mediante la metrica della disponibilità del servizio.

Essa è misurata in base ai due parametri di Uptime (Tempo ininterrotto di disponibilità di un servizio) e MTBF (Mean Time Between Failures, tempo che intercorre tra due guasti consecutivi dello stesso servizio).

La disponibilità di base richiesta è di 24 ore al giorno e 365 giorni l'anno.

I valori richiesti sono i seguenti:

1. Uptime > 99,8%
2. MTBF > 2000 ore

Si noti che il parametro di Uptime è comprensivo anche degli interventi, con caratteristiche bloccanti del servizio, programmati per finalità di manutenzione preventiva e/o evolutiva.

Si richiede che eventuali interruzioni di servizio per manutenzioni siano comunicate con un anticipo di almeno 3 giorni.

3 Documentazione tecnica di progetto

Deve essere presentata una relazione tecnica che descriva l'architettura del Servizio che si intende realizzare.

Esso deve consistere in una descrizione dei Siti proposti illustrandone:

- la posizione geografica all'interno delle città (indirizzo completo di piano di ubicazione)
- la pianta dei locali con indicazione chiara della posizione proposta per l'allocazione degli EPO-LP, indicando anche quanto presente in termini di attrezzature negli stessi locali
- l'attrezzaggio tecnologico in termini di infrastrutture civili (p. es. pavimento flottante), energia elettrica ed UPS, condizionamento etc.
- regolamento proposto per l'accesso e l'utilizzo dei locali
- Documento Programmatico di gestione della sicurezza

Tecnopolis CSATA

Regione Puglia

Rete Unitaria della Pubblica Amministrazione Regionale

(R.U.P.A.R)

Modulo di adesione delle Amministrazioni Locali alla RUPAR

(prodotto nell'ambito della Convenzione approvata dalla Giunta Regionale con deliberazione n. 1162 del 10/8/2001)

Allegato F

Versione 2.0 del 18/7/2002

Modulo di adesione alla RUPAR

(indirizzato dall'Amministrazione Locale che aderisce a RUPAR alla Regione Puglia)

[Carta intestata dell'Amministrazione]

Il sottoscritto: _____

Legale rappresentante dell'Amministrazione: _____

Con sede in: _____ via/P.za _____N°.___ CAP_____

Cod. Fiscale: _____ tel: _____ fax: _____

DICHIARA

Di voler aderire alla RUPAR Puglia realizzata dalla Regione Puglia mediante la Misura 6.3, Sottomisura A, Azione a) del POR 2000-2006.

Di essere a conoscenza che detta Azione provvede al finanziamento pubblico dell'iniziativa per il 50% del valore corrispondente alla classe di servizio prevista per l'Amministrazione e prevede che il restante 50% sia a carico dei Fornitori che realizzano il servizio.

Di essere a conoscenza del sistema completo di servizi fornito dalla RUPAR Puglia e che la classe di servizio prevista per l'Amministrazione richiedente, intesa come:

- Ampiezza di banda del collegamento per il Servizio di Trasporto
- numero di Posti di Lavoro (PdL) gestiti per il Servizio di Interoperabilità di base
- numero di certificati di firma per il Servizio di Firma Digitale

è legata al numero dei dipendenti dell'Amministrazione secondo le seguenti relazioni:

- Numero PdL = 1/3 x Numero dei dipendenti (arrotondato all'unità in eccesso)
- Numero certificati di Firma Digitale = 1/2 x Numero dei Posti di lavoro (arrotondato all'unità in eccesso)
- Ampiezza di banda del collegamento dipendente dal numero di PdL in funzione della seguente tabella:

Numero **n** di PdL	**Ampiezza di banda (Kbps)**
n ≤ 25	64
25 < n ≤ 50	128
50 < n ≤ 100	256
100 < n ≤ 250	384
250 < n ≤ 500	512
500 < n ≤ 1000	768
N > 1000	2048

Che il Numero dei Dipendenti dell'Amministrazione è pari, alla data odierna, a: Euro_____ unità.

Di essere a conoscenza che tutte le informazioni formali, tecniche ed economiche relative alla RUPAR ed alle modalità operative con essa è realizzata, ivi inclusi:

- copia della Delibera della Giunta Regionale n. 1162 del 10/8/2001
- il Piano Strategico della RUPAR
- i Capitolati Tecnici di qualificazione dei Fornitori
- l'elenco dei Fornitori qualificati
- il Costo di Riferimento per i servizi RUPAR
- il Costo di Riferimento per i servizi aggiuntivi strettamente connessi ai servizi RUPAR

sono disponibili sul sito della RUPAR Puglia all'indirizzo http://www.rupar.puglia.it

Che l'eventuale ricorso ai servizi aggiuntivi è a proprio totale carico.

SI IMPEGNA

A nominare il sig. _____ tel. _____, fax. _____ email:_____ come proprio referente per gestire i contatti relativi alla RUPAR con la Regione Puglia, il Centro Tecnico della RUPAR, i Fornitori e le altre Amministrazioni.

A richiedere il servizio RUPAR esclusivamente ad uno dei Fornitori qualificati il cui elenco è disponibile sul sito della RUPAR.

A comunicare, ai fini della corretta gestione della sicurezza della RUPAR, entro 30 giorni dalla data attuale, alla Regione Puglia e al Centro Tecnico della RUPAR eventuali collegamenti dati già esistenti con la rete Internet e/o con altre organizzazioni.

A non attivare, in aggiunta al collegamento a RUPAR, ulteriori collegamenti con la rete Internet.

A richiedere, in caso di necessità, servizi aggiuntivi consistenti nell'innalzamento della classe di servizio prevista per l'Amministrazione (p. es. maggiore velocità del collegamento o maggior numero di PdL) esclusivamente al Fornitore RUPAR prescelto.

A richiedere, in caso di necessità, servizi aggiuntivi strettamente connessi al servizio RUPAR e precisamente:

- attivazioni di VPN (Virtual Private Network) sulla Porta di Rete (PdR) della RUPAR
- gestione dell'indirizzamento, dei nomi e della sicurezza a livello Firewall di elaboratori di servizio attivati sulle reti di servizio DMZ e RSR dell'Amministrazione
- attivazione di ulteriori dispositivi di lettura di Smart Card della Firma Digitale
- attivazioni di ulteriori servizi sulle smart card della Firma Digitale

esclusivamente al Fornitore RUPAR prescelto.

Ad osservare le raccomandazioni del Centro Tecnico della RUPAR, pubblicate sul sito RUPAR Puglia, relativamente all'utilizzo dei Servizi nonché alle modalità di attuazione ed attivazione su RUPAR di servizi di cooperazione applicativa con altre Amministrazioni e/o di servizi applicativi per le altre Amministrazioni e per i cittadini.

A rendicontare alla Regione Puglia le spese coperte dal finanziamento regionale secondo le regole di rendicontazione previste dal POR, utilizzando la procedura informatica resa disponibile dal Centro Tecnico sul suo sito Web.

Data, _____ [Timbro e Firma]