ASSESSORATO ALL’UNIVERSITA’ E RICERCA SCIENTIFICA, INNOVAZIONE TECNOLOGICA E NUOVA ECONOMIA, SISTEMI INFORMATIVI E STATISTICA, MUSEI E BIBLIOTECHE

DISCIPLINARE TECNICO

Appalto-concorso per la realizzazione del Sistema Regionale per la Cooperazione Applicativa in Sicurezza

---

Bollettino Ufficiale della Regione Campania Numero 25 del 9 maggio 2005

Decreto Dirigenziale n. 302 del 21 aprile 2005
Indizione della gara per Appalto-concorso finalizzata alla realizzazione del Sistema Regionale per la Cooperazione Applicativa in Sicurezza e contestuale approvazione degli atti prodomici.

Indice

Premessa

L’oggetto del presente disciplinare tecnico è la descrizione delle specifiche tecniche per la realizzazione di un “Sistema Regionale per la Cooperazione Applicativa in Sicurezza, inteso come piattaforma abilitante, operante in sicurezza, per gestire l’accesso ai servizi offerti dai diversi Enti connessi in una rete geografica di tipo sia extranet che internet, nonché nei servizi di conduzione, manutenzione, nulla escluso, del Sistema per la durata di 3 (tre) anni, a far data dall’avvenuto positivo collaudo.

La fornitura dovrà comprendere e garantire:

a) La realizzazione di una piattaforma (Sistema) che implementi le specifiche funzionali per la gestione dei servizi previste dal “Nodo Aggregatore” (NAG) definito nel modello Sistema Pubblico di Interoperabilità e Cooperazione applicativa Campana (SPICCA) della Regione Campania, che identificano:
   - le funzionalità dei servizi di base necessari affinché diversi Enti ed Amministrazioni dotati di infrastrutture informatiche e telematiche proprie possano scambiare informazioni fra loro in modo controllato;
   - le modalità per la cooperazione applicativa, ossia la possibilità di realizzare servizi ed automatizzare processi impiegando funzionalità coordinate di più infrastrutture.

La piattaforma oggetto della presente gara deve implementare le funzioni base per la cooperazione applicativa del “Nodo Aggregatore” (NAG) definito nel modello SPICCA della Regione Campania.
Precisamente le funzioni base sono:

- accesso a servizi, usufruibili mediante una semplice interfaccia web e/o applicativi che richiedono in modo automatico l’attivazione dei servizi;
- ricerca e indicizzazione dei servizi;
- implementazione di politiche di sicurezza che consentano di discriminare l’accesso sia all’indice dei servizi che alle diverse funzionalità da questi previste;
- accesso da diverse tipologie di terminali fissi e mobili (telefoni cellulari WAP o UMTS, personal computer, laptop, palmari, etc).

In aggiunta alla realizzazione delle funzioni di base per la cooperazione applicativa, la fornitura prevede la realizzazione delle funzioni specifiche del nodo per l’aggregazione relativo al Centro di Prenotazione Unico (CUP) sanitario della Regione Campania. Il nodo, ottenuto integrando i servizi di prenotazione disponibili presso le ASL e le aziende ospedaliere, deve fornire un servizio di prenotazione integrato su tutte le disponibilità presenti in Campania. Tale attività è una concreta sperimentazione delle funzionalità del NAG per uno specifico servizio e si avvarrà dei risultati del progetto di adeguamento dei CUP degli Enti sanitari finanziato dalla Regione Campania, che ha consentito alla ASL e alle Aziende Ospedaliere di omogeneizzare i propri sistemi di prenotazione.
Le funzioni base del Nodo Aggregatore e le funzioni specifiche relative al sistema CUP devono essere realizzate in due architetture fisicamente distinte che possano essere allocate in due diversi punti di accesso della rete della Regione Campania.
I servizi da integrare saranno resi disponibili per ogni Ente coinvolto in due diverse modalità tramite: pagine web e accesso basato su tecnologie di tipo “web services”; per entrambe le modalità deve essere prevista l’integrazione nel NAG.
Si fa presente che gli Enti coinvolti nel CUP devono poter continuare ad offrire i propri servizi in autonomia indipendentemente dalle funzionalità previste per il nodo aggregatore.

La piattaforma da realizzare deve soggiacere ai seguenti vincoli generali:

1. La piattaforma sarà per tutti i componenti hardware e software di proprietà della Regione Campania;

2. La realizzazione della piattaforma prevede la fornitura di tutti i componenti hardware e software; tali componenti devono essere allocati all’interno della struttura della Regione Campania e devono soddisfare i livelli di servizio individuati in questo capitolato. Soluzioni che limitano lo spazio fisicamente occupato da tutti i componenti (ad esempio con l’uso di armadi rack) sono da preferire.

3. La piattaforma deve operare in sicurezza, in particolare devono essere forniti diversi meccanismi di autenticazione ed autorizzazione deboli e forti che prevedano l’impiego di dispositivi smart-card compatibili con la carta di identità elettronica e/o con una carta servizi. Tutti gli adeguamenti non devono prevedere alcun costo aggiuntivo per tutto il periodo della fornitura;

4. La piattaforma deve operare: sulla Extranet e sulla Intranet della Regione Campania, in Internet e deve inoltre poter operare in ogni sistema di rete che sia conforme alle specifiche del Sistema Pubblico di Connettività (SPC);

5. La gestione dell’intera piattaforma è a cura della società che la realizzerà per il periodo oggetto della fornitura; la gestione dei profili di sicurezza, della loro modifica o aggiornamento è a cura della Regione Campania;

6. Devono essere recepite tutte le specifiche tecniche e gestionali definite in sede nazionale ed internazionale, ed in particolare quelle sulla cooperazione applicativa definite e in corso di definizione dal CNIPA o dal Ministero dell’Innovazione Tecnologica, nonché le direttive tecniche e gli standard definiti dal consorzio internazionale *W3C*. Tutti gli adeguamenti non devono prevedere alcun costo aggiuntivo per tutto il periodo della fornitura;

7. Il formato dei dati e i protocolli tra i sistemi deve essere conforme a quanto stabilito dalle specifiche tecniche sulla “Busta di E-government”, così come definita dalla Presidenza del Consiglio dei Ministri in relazione ai progetti di e-Government nazionali. Tutti gli adeguamenti non devono prevedere alcun costo aggiuntivo per tutto il periodo della fornitura.

8. Il sistema sia per quanto attiene l’indicizzazione dei servizi che per quanto attiene la gestione degli accessi in sicurezza deve poter operare in maniera federata con i sistemi di altri Enti, anche secondo quanto previsto dal modello SPICCA. Ne deriva che il sistema di indicizzazione dei servizi deve poter essere puntato o puntare ad altri sistemi di indicizzazione ed il sistema di controllo accessi deve poter operare in collaborazione con altri sistemi di controllo accessi, per garantire l’accesso in modo integrato a servizi di diversi enti con livelli di sicurezza predefiniti;

9. Tutte le modalità di funzionamento e interazione tra sistemi devono avvenire utilizzando protocolli e formati dati rispondenti a standard di mercato aperti e consolidati;

10. Il sistema deve essere estremamente modulare: ogni singola funzionalità del sistema deve essere accessibile sia in modo autonomo che in modo integrato nella piattaforma e deve essere possibile la sostituzione di un componente con uno funzionalmente equivalente

senza alcuna modifica della restante parte dell’architettura. La modularità va intesa anche come scalabilità delle prestazioni del sistema.

11. Il sistema dovrà essere in linea con le esigenze della Stazione Appaltante, descritte dettagliatamente nella metodologia adottata con il modello SPICCA ed in accordo alle politiche di Riuso della Regione Campania. Pertanto il sistema dovrà essere scalabile, flessibile, modulare e riusabile, nel senso che le componenti sw costituenti l’architettura dovranno poter essere il più possibile condivisibili e riutilizzabili da più Amministrazioni e devono poter operare su diverse architetture informatiche. Il modello SPICCA prevede infatti l’impiego di soluzioni basate su standard aperti e su soluzioni architetturali che possono essere, anche in futuro, utilizzate da più nodi di dominio e nodi aggregatori.

b) Conduzione del Sistema per 3 (tre) anni a partire dall’avvenuto positivo collaudo;
c) Manutenzione sia preventiva che a richiesta, del Sistema per tre (tre) anni a partire dall’avvenuto positivo collaudo;
d) Nomina di un responsabile di progetto per ogni tipologia di servizi richiesti dal presente capitolato, inclusa la gestione della sicurezza, le cui note curriculari devono comprovare le referenze richieste nel disciplinare;
e) Almeno 600 (seicento) ore di training on the job e 600 (seicento) ore di formazione in aula del personale utilizzatore del Sistema. L’Ente si riserva la facoltà di ridistribuire le sopraccitate ore in modo diverso da quello stabilito;
f) Assistenza operativa alla Stazione Appaltante nella sperimentazione e/o nello sviluppo di servizi innovativi nell’ambito delle funzionalità previste dal presente capitolato tecnico, fornendo anche consulenza sulla piattaforma realizzata agli Enti individuati dalla regione per effettuare la sperimentazione.

La definizione delle specifiche tecniche della piattaforma e dei suoi ambiti applicativi è indicata nelle seguenti sette sezioni:

1. Architettura di riferimento (vedi Capitolo 1); in questa sezione verranno descritti i requisiti dell’architettura ed il modello di riferimento per la realizzazione del sistema Regionale per la Cooperazione Applicativa in sicurezza;
2. Funzionalità per la realizzazione della Piattaforma (vedi Capitolo 2); in funzione dei requisiti descritti nel Capitolo 1, in questa sezione verranno descritte le funzionalità che la piattaforma dovrà garantire per offrire servizi di cooperazione applicativa operanti in sicurezza;
3. Componenti della piattaforma (vedi Capitolo 3); in questa sezione verranno descritte le componenti necessarie per garantire tutte le funzionalità del sistema; le componenti verranno descritte dettagliatamente in modo tale che esse possano essere utilizzate sia singolarmente che in modo integrato;
4. Scenari d’uso (vedi Capitolo 4); in questa sezione verranno descritti, a titolo esemplificativo, alcuni possibili scenari d’uso della piattaforma, con particolare attenzione alle modalità di controllo degli accessi;
5. Servizio aggregatore per il sistema CUP della Regione Campania (vedi Capitolo 5); in questa sezione verranno descritti, a titolo esemplificativo, alcuni possibili scenari d’uso della piattaforma con esplicito riferimento alla sperimentazione del sistema CUP.
6. Livelli di servizio (vedi Capitolo 6); in questa sezione verranno descritti i parametri quantitativi e qualitativi che caratterizzano la qualità dei servizi offerti dal NAG e della fornitura stessa.

7. Attività di supporto alla realizzazione del progetto (vedi Capitolo 7); in questa sezione vengono riportate alcune informazioni relative alla gestione e manutenzione del sistema e alla formazione del personale.

Si precisa che, in ottemperanza alla strategia adottata dalla Regione Campania, meglio espressa, per il progetto de quo, nella metodologia SPICCA (Sistema Pubblico per l’Interoperabilità e la Cooperazione applicativa CAmpana), che prevede di realizzare architetture applicative condivisibili e riutilizzabili da più Amministrazioni, la Ditta dovrà garantire, e quindi documentare, una soluzione caratterizzata anche dal paradigma dello sviluppo software Open Source, allo scopo di estendere il più possibile la riusabilità senza oneri aggiuntivi per l’Amministrazione. Quindi, si precisa che imprescindibilmente, a pena esclusione, almeno le componenti software riguardanti la realizzazione della busta di e-Gov e del Proxy applicativo per l’accesso alle risorse e/o servizi esposti da un dominio interoperante dovranno essere di tipo Open Source, che potrà essere o riadattato, o realizzato ex novo ad hoc (sempre secondo il paradigma dell’Open Source) per la Stazione Appaltante, poiché le stesse dovranno essere replicate su altri nodi dell’architettura cooperativa, per cui è necessario che siano di proprietà della Stazione Appaltante. All’occorrenza, per i sopraccitati componenti software di tipo open source, la Ditta dovrà, oltre che produrre tutta la documentazione prevista per legge, consegnare il codice sorgente per permettere alla Stazione Appaltante di poter intervenire con ogni tipo di adattamento idoneo a soddisfare le proprie esigenze e, nel contempo, permettere alla stessa Amministrazione di poter procedere al riuso delle soluzioni su architetture diversificate. Il fine è quello di consentire all’Ente Committente il pieno sfruttamento, in termini di modularità, flessibilità, estensibilità, replicabilità e riusabilità su diverse piattaforme della soluzione, degli antescritti moduli software, coerentemente con la politica del Riuso propria della strategia regionale in materia.

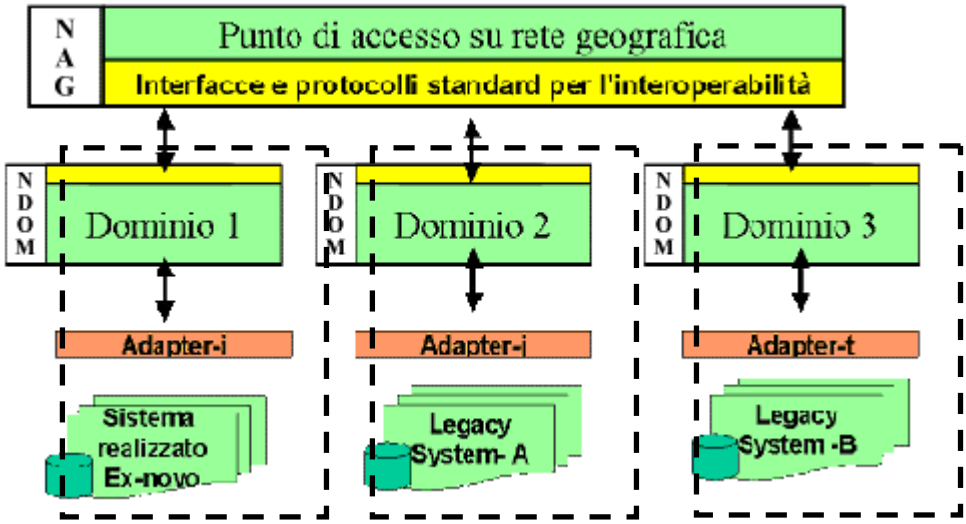
1 Architettura di riferimento

Con riferimento al modello SPICCA viene presentata una architettura modulare di riferimento per ottenere funzionalità di cooperazione spinta tra servizi offerti da diversi enti, preservando l’autonomia e la peculiarità dei singoli sistemi interconnessi.
Un modello logico di riferimento di elaborazione distribuita è rappresentato nella Figura seguente, dove ogni singola infrastruttura informatica dei diversi Enti è vista come un dominio unitario vincolato a meccanismi standard di interfacciamento.
Per poter garantire l’interfacciamento, ogni dominio può utilizzare una specifica unità con funzione di *adapter*, il cui compito è rendere disponibili, secondo le modalità di interazione definite, i sevizi già attivi e funzionanti presso lo specifico Ente.

Nel sistema sono presenti due tipologie di nodi funzionali:

- **Nodi di Aggregazione** (NAG) per la integrazione e gestione di servizi di supporto all’interoperabilità:
    1. ***Presentazione di un servizio:*** dal punto di vista di un utente che vuole accedere alla piattaforma, tale nodo deve presentare sia la funzione di rendere omogenei e integrati servizi offerti da diversi Enti per offrire uno stesso servizio su più ampia scala (ad esempio, servizi anagrafici offerti da diversi comuni), che di integrare mediante interfaccia standard diverse tipologie di servizi per offrire un nuovo servizio complesso a valore aggiunto (ad esempio integrazione di banche dati di competenza di diversi Enti per fornire servizi).
    2. ***Broker di servizi:*** dal punto di vista di un Ente generico, tale nodo deve rappresentare il punto a cui si può accedere per richiedere un servizio e il punto in cui più servizi possono essere integrati. Questo significa che un NAG può aggregare sia servizi appartenenti a diversi Enti che diverse strutture/servizi di uno stesso Ente, inoltre, grazie a tale funzione, un NAG deve provvedere ad un effettivo bilanciamento del carico.

  In definitiva, il NAG deve supportare sia utenti esterni “presentando” loro un ambiente unico di accesso, sia altri Enti per la cooperazione applicativa. Ovviamente, i nodi di aggregazione possono essere visti a loro volta come nodi oggetto di ulteriore aggregazione (nodi che possono operare in modo federato);
- **Nodi di dominio** (NDOM) per l’accesso ai servizi applicativi di un Ente, che integrano eventuali sistemi di adattamento, inclusa la presenza di eventuali adapter o connettori ai sistemi informatici locali agli Enti. Tali nodi possono offrire servizi in modo autonomo e/o attraverso nodi di aggregazione.



Modello logico di riferimento

Per perseguire gli obiettivi occorre dunque definire una infrastruttura complessa sia dal punto di vista tecnico che organizzativo, che sia in grado di soddisfare in maniera efficiente le esigenze specifiche degli Enti coinvolti che hanno necessità di accedere a servizi applicativi distribuiti offerti da altri Enti. Nella sua complessità, tale infrastruttura deve essere in grado di:

- offrire servizi applicativi nel modo più semplice ed efficace possibile,
- mascherare l’eterogeneità e la distribuzione dei servizi applicativi,
- proteggere sistemi e dati riservati,
- gestire l’accesso alle risorse condivise,
- monitorare la qualità dei servizi NAG e dei nodi NDOM.

Ne deriva che il nodo aggregatore può essere visto come composto da due macro componenti:

- una di supporto base alla cooperazione di tipo strutturale (Servizio di Registry, Servizio di Logging, Servizi di monitoraggio del workflow, Servizi di Sicurezza);
- una con funzioni più significativamente legate alla gestione dei particolari servizi di riferimento, che va di volta in volta realizzata per la specifica applicazione.

Ovviamente non saranno sempre presenti le due componenti per tutte le tipologie di servizi. La funzione del nodo aggregatore potrà essere quindi semplicemente quella di supporto all’interoperabilità in sicurezza, limitandosi ad esempio alla sola pubblicazione di servizi di competenza di nodi di dominio o di altri nodi aggregatori. Nel progetto del sistema le due macro componenti devono operare in modo indipendente sia dal punto di vista logico che fisico e la realizzazione delle funzioni di supporto alla cooperazione devono essere utilizzabili per l’aggregazione di qualsiasi servizio applicativo.

La realizzazione delle funzioni di supporto base alla cooperazione e di quelle relative alla realizzazione del nuovo Centro di Prenotazione Unica (CUP), ottenuto per aggregazione di servizi esistenti, rientra negli obiettivi del presente capitolato.

Le funzioni base del Nodo Aggregatore e le funzioni specifiche relative al sistema CUP devono essere realizzate in due architetture fisicamente distinte che possano essere allocate in due diversi punti di accesso della rete della Regione Campania. Di seguito vengono presentate prima le caratteristiche dell’architettura per la realizzazione delle funzioni base del nodo aggregatore e in un successivo capitolo quelle per la realizzazione del sistema CUP.

Le strategie da implementare per la realizzazione del sistema sopra illustrato includono:

- applicazione di standard per il formato dei documenti e dei dati trasmessi;
- scelta di metodologie e standard per l’invocazione remota di funzioni disponibili in altri domini applicativi tenendo conto delle problematiche di sicurezza;
- connessione tra i sistemi;
- metodi standard per indicizzare ed interrogare le modalità di accesso ai servizi applicativi ed alle risorse.

Il **NAG** è un *aggregatore* di servizi ossia un elemento di *intermediazione*. I servizi per la cooperazione possono essere differenti in funzione del modello di cooperazione scelto; i modelli attualmente più diffusi sono SOA (Service Oriented Architecture) ed EDA (Event Driven Architecture) e devono essere entrambi supportati. Questi offrono *l'opportunità agli intermediari di costruire nuovi servizi aggregandone degli altri*. Il nuovo servizio può raggruppare i servizi che vengono forniti da diversi **NDOM**. Il nodo NAG, come già evidenziato, può avere solo la funzione di nodo di supporto ai servizi cooperativi.

Riprendendo quanto già sinteticamente illustrato sia ha che le caratteristiche di un NAG che si propone come aggregatore di servizi sono:

- assicurare la fruibilità dei servizi esposti;
- fornire un ambiente transazionale e sicuro;
- garantire e monitorare la 'quality of service' dei servizi applicativi (anche quando il servizio è realizzato con la cooperazione di più Enti);
- prevenire o gestire situazioni critiche come attacchi (ad esempio il “denial of service”) o guasti.

Il **NAG** svolge anche il ruolo di **broker** per mantenere la descrizione dei servizi che vengono erogati dal NAG stesso e dagli NDOM che partecipano alla cooperazione applicativa. Il NAG e ogni NDOM svolgono anche il ruolo di **requestor** rispetto a tutti gli altri NDOM che a loro volta offrono la possibilità di eseguire l'aggregazione di contenuti e servizi ai loro clienti.

I servizi di un NAG, consentono ad un generico requestor (sia esso un utente esterno o un Ente) di:

- localizzare il servizio migliore, in termini di efficienza o di costo (nell’ottica del raggiungimento di un determinato livello di qualità);
- scegliere tra servizi alternativi, dato che un requestor non ha nessun controllo sulla disponibilità dei servizi offerti dagli altri nodi;
- fruire di un ambiente sicuro.

Gli **NDOM**, a loro volta, vengono visti come centri di '*business process*', ossia espongono i servizi applicativi che devono essere opportunamente indicizzati indipendentemente dal modello cooperativo prescelto (SOA, EDA). I servizi applicativi devono accedere ad un insieme di

applicazioni in grado di eseguire l’intero processo di business (attraverso lo strato che garantisca la *presentazione*).

In ogni caso per consentire la piena autonomia ai nodi di dominio è importante evidenziare che i servizi offerti da un NDOM possono essere acceduti anche direttamente senza utilizzare gli eventuali Adapter e continuando ad utilizzare i meccanismi locali di controllo degli accessi.

1.1 Modularità e Scalabilità del Sistema

Una delle caratteristiche dell’architettura deve essere quella di avere la capacità di adeguarsi alla nascita di nuove necessità, ossia deve garantire la possibilità di ampliare l’insieme dei servizi offerti estendendo il sistema nel suo complesso senza variare il modello di gestione.

Il sistema deve dunque essere modulare; in tale contesto la modularità va intesa nella triplice accezione:

1. ogni singola funzionalità del sistema deve essere accessibile sia in modo autonomo che in modo integrato nella piattaforma.
2. la sostituzione di un componente con uno funzionalmente equivalente deve avvenire senza alcuna modifica della restante parte dell’architettura.
3. la possibilità di accrescere le prestazioni del sistema deve avvenire aggiungendo nuovi componenti o ridondando quelli già esistenti.

La piattaforma deve essere fondata su un’architettura aperta, ossia basata su tecnologie e standard le cui specifiche siano disponibili indipendentemente dalla scelta implementativa (hardware, software, linguaggi di programmazione,…).
In tale contesto la scalabilità del sistema deve essere vista anche come requisito architetturale dato che sia gli Enti che offrono servizi che i nodi aggregatori devono cooperare nello stesso modo con cui i nodi terminali di vari domini cooperano tra loro.

1.2 Prestazioni ed Affidabilità del Sistema

La piattaforma ipotizzata, per sua natura, è soggetta ad un elevato carico ed a possibili attacchi nocivi che possono compromettere il corretto funzionamento o l’integrità del sistema nel suo insieme; tali fattori di rischio possono contribuire a situazioni tipo “Denial of Service” (negazione di servizio), quindi occorre progettare meccanismi che garantiscano il funzionamento del sistema in ogni condizione e garantiscano le prestazioni indicate nel paragrafo sui livelli di servizio.
I meccanismi necessari per garantire l’affidabilità del sistema, devono basarsi su tecniche di replicazione temporale e/o spaziale dei componenti hw e/o sw.

2 Funzionalità per la realizzazione della piattaforma

Data l’architettura di riferimento, le funzionalità che la piattaforma deve offrire sono riconducibili alla seguente classificazione:

- Funzionalità per l’integrazione e l’interoperabilità;
- Funzionalità per la gestione della sicurezza;
- Funzionalità per la gestione dell’accesso multicanale da dispositivi eterogenei;
- Funzionalità di tracciabilità;
- Funzionalità di monitoraggio della qualità dei servizi;

Nei prossimi sottoparagrafi vengono descritte nel dettaglio le singole funzionalità.

2.1 Funzionalità per l’integrazione e l’interoperabilità

Per quanto ampiamente illustrato in SPICCA; alla base della cooperazione applicativa è necessario definire un modello di cooperazione tra servizi. L’architettura di riferimento deve permettere l’utilizzo sia di modelli di cooperazione per eventi (EDA) che quelli per invocazione di servizi (SOA), ampiamente descritti in letteratura. Questi modelli hanno la necessità di usare delle funzionalità di base per la pubblicazione, indicizzazione, ricerca/individuazione e presentazione dei servizi.
Le funzionalità individuate che devono essere garantite qualunque sia il modello cooperativo, sono:

- Servizi di pubblicazione;
- Servizi di indicizzazione e ricerca ;
- Servizi di presentazione e integrazione;
- Servizi di supporto alla cooperazione.

Tutti i servizi devono essere erogati garantendo la correttezza delle transazioni effettuate, dove la transazione è intesa come sequenza di operazioni da eseguire in modo atomico. Il mancato completamento di una transazione deve essere supportato da processi di roll-back che devono annullare tutti i cambiamenti effettuati dalla transazione abortita, e riportare lo stato del sistema nelle identiche condizioni di partenza.

Servizi di pubblicazione
Un Ente che intende offrire un servizio deve poter rendere pubblica la locazione dello stesso e/o la sua descrizione in termini di descrizione delle funzionalità offerte e delle modalità di accesso con riguardo anche al formato dei dati utilizzati. Il meccanismo utilizzato deve consentire lo sviluppo di applicazioni software che richiedano in modo automatico l’ utilizzo dei servizi offerti.

Servizi di indicizzazione e ricerca
La capacità di rintracciare, facilmente ed in maniera dinamica, servizi offerti da possibili Enti, è un requisito fondamentale. Un Ente può invocare i servizi di altri per eseguire le transazioni di cui necessita. In uno scenario in cui solo pochi Enti partecipano, gestire la ricerca può essere semplice; la ricerca si complica notevolmente man mano che il numero di Enti e/o servizi che interagiscono cresce, è dunque necessario un servizio di indicizzazione e ricerca che può essere gestito mediante uno o più registri, eventualmente gestiti da più Enti, dedicati alla pubblicazione dei servizi.

Servizi di presentazione e integrazione
L’accesso ai servizi può avvenire sia da altre applicazioni software che da utenti che si possono connettere con diversi dispostivi. Esistono pertanto due problematiche di presentazione legate a:

- L’impiego di meccanismi software tali che, usando opportune modalità di accesso e un opportuno formato dati, consentano ad altre applicazioni software di collegarsi automaticamente ai servizi basandosi su tecnologie e standard aperti ampiamente sviluppati.

- La realizzazione di sistemi per l’accesso da terminali eterogenei, tema di notevole interesse ed in continua evoluzione con la diffusione crescente di sistemi di elaborazione mobile e di telefonia.

I dispositivi si differenziano per caratteristiche quali la risoluzione del display, la tecnologia di comunicazione, le risorse di calcolo e di memoria.
Risulta quindi necessario un servizio di presentazione che si occupi di rappresentare l'interfaccia del servizio per un particolare dispositivo.
Per garantire l’interoperabilità, devono essere recepite o recepibili tutte le specifiche tecniche e gestionali sulla cooperazione applicativa definite dal CNIPA o dal Ministero dell’Innovazione Tecnologica, nonché le direttive tecniche e gli standard definiti dal consorzio internazionale *W3C*.

Servizi di supporto alla cooperazione.

Per la definizione di servizi aggregati a valore aggiunto e per rendere effettiva la cooperazione tra i servizi applicativi, è necessario definire un modello di cooperazione tra servizi.
L’architettura di riferimento deve offrire servizi di base per realizzare sia modelli di cooperazione per eventi (Event Driver Architecture) che quelli per invocazione di servizi (Service Oriented Architecture), ampiamente descritti in letteratura.

2.2 Funzionalità per la gestione della sicurezza

La sicurezza gioca un ruolo fondamentale in tutta l’infrastruttura; il sistema deve essere in grado di fornire non solo meccanismi che proteggano l’infrastruttura e le singole risorse/servizi da utenti maliziosi o semplicemente non autorizzati (identificazione ed autorizzazione), ma anche meccanismi in grado di monitorare le attività di un utente nell’accesso ad un servizio (monitoring ed auditing) con la gestione di opportune attività di Intrusion Detection e logging.

Tutti i componenti dell’architettura in grado di offrire questa funzionalità, devono includere:
- Servizi di controllo degli accessi,
- Servizi di certificazione,
- Servizi di monitoraggio ed auditing,
- Servizi di Logging.

Per proteggere le applicazioni e le risorse, occorre implementare dei servizi che permettano:

- identificazione ed autenticazione di utenti/Enti e componenti del sistema;
- controllo degli accessi (autorizzazione);
- auditing e monitoring.

L’identificazione è il processo attraverso il quale una risorsa dichiara la propria identità nell’ambito di un sistema o di un’applicazione.
L’autenticazione è il processo attraverso cui, in una comunicazione tra due parti (uomo-macchina, macchina-macchina, uomo-applicazione, applicazione-macchina, ecc…), una parte verifica la veridicità dell’identità conclamata dall’altra parte.
L’autorizzazione è il processo attraverso cui ad un utente, preventivamente autenticato, viene assegnato un permesso di utilizzo di una o più risorse.
L’auditing, ed il monitoraggio (intrusion detection e monitoraggio delle possibili rischi di attacco al sistema) implementano il processo attraverso cui risulta possibile controllare i punti critici del sistema e tentativi di attacco.

Un’attenzione particolare merita il discorso sulla gestione della sicurezza all’interno della federazione di nodi, dato che servizi aggregati potrebbero coinvolgere NDOM appartenenti a domini di sicurezza diversi con politiche di accesso diverse, sia per le regole espresse che per i ruoli ed i profili definiti.
Politiche di domini diversi appartenenti a servizi che devono cooperare, potrebbero essere in conflitto tra loro e ciò potrebbe causare notevoli problemi di sicurezza ad esempio legati alla “escalation di privilegi” di utenti non autorizzati.
Tali problemi devono essere assolutamente affrontati sia in termini tecnologici (prevedendo funzionalità automatiche di policy-mapping e cross-certification tra domini) che organizzativi (prevedendo che in fase di registrazione di un nuovo servizio aggregato la Service Registration Authority si occupi esplicitamente di verificare la compatibilità delle policy e dei meccanismi di sicurezza).

2.3 Funzionalità per la gestione dell’accesso multicanale da dispositivi eterogenei

Il sistema deve consentire l’accesso ai servizi da terminali client di diversa natura utilizzando, ove necessario, tecniche di adattamento per i diversi dispositivi coinvolti, inoltre la piattaforma dovrà supportare le diverse tecnologie di rete attualmente disponibili.

Data la eterogeneità dei canali e dei protocolli di accesso, è necessario prevedere dei servizi che si occupino della gestione delle diverse tecnologie di rete in maniera del tutto trasparente all’utente.
La piattaforma dovrà supportare le diverse tecnologie di rete attualmente disponibili; i servizi devono prevedere sia le modalità di accesso di tipo tradizionale (accesso ad internet, portali web, e-commerce,…) che quelle di nuova generazione (UMTS).

Per l’accesso multicanale, la necessità di dover gestire terminali eterogenei, richiede la disponibilità del seguente set minimale di protocolli di accesso:

- WAP
- HTTP
- HTTPS
- SOAP

Per ogni protocollo utilizzato deve essere possibile l’accesso differenziato ai servizi disponibili nel sistema.
Per quanto riguarda l’eterogeneità del canale di accesso, tutti i componenti dell’architettura in grado di offrire questa funzionalità, devono includere servizi orientati a tecnologie wired e wireless.

2.4 Funzionalità per la Tracciabilità

La cooperazione di una moltitudine di Enti, soggetti e sistemi, in uno scenario distribuito in cui i servizi forniti possono rivestire un ruolo di elevata criticità, pone la problematica di dover tracciare operazioni e transazioni effettuate da ogni possibile attore che opera all’interno dell’intero sistema.
Per quanto detto devono prevedersi funzionalità di tracciabilità sia degli utenti che dei sistemi gestibili in modo centralizzato.
Opportuni sistemi di logging devono operare al fine di tracciare ogni operazione di rilievo per i sistemi locali di ogni dominio, per poi inoltrare tali dati ad un servizio centralizzato operante nel NAG.
L’identità degli operatori tracciati deve essere fortemente integrata al sistema di autenticazione dei soggetti e del controllo degli accessi, garantendo assoluta consistenza tra l’identità dei soggetti ed i dati di log di tracciamento archiviati.
I dati relativi alla tracciabilità devono poter essere utilizzati per ricondurre in modo inequivocabile ai soggetti attuatori le operazioni da essi eseguite.
Opportuni sistemi di analisi e consultazione di tali dati devono essere impiegati nel sistema centralizzato di gestione della tracciabilità.

2.5 Funzionalità per il Monitoraggio operativo della qualità dei servizi

La complessità del sistema presenta la necessità di implementare funzionalità e meccanismi di controllo atti a vigilare l’operato di ogni nodo interoperante al fine di garantire il raggiungimento di apprezzabili livelli qualitativi nella fornitura dei servizi erogati.

Per evitare il degradamento degli standard qualitativi, il sistema deve garantire attraverso opportuni apparati di controllo, il monitoraggio della qualità dei servizi attesi rispetto a ben definite soglie di riferimento che devono essere pubblicate e documentate per ogni singolo servizio. Tali dati devono essere esposti ed accessibili sul NAG, e con essi le metriche di valutazione relative.
Gli apparati preposti al monitoraggio, avvalendosi di opportuni meccanismi e dispositivi di rilevamento dei livelli di servizio erogati, devono riportare i dati rilevati, ed eventuali violazioni dei livelli attesi; in un sistema centralizzato di monitoraggio tali apparati devono essere residenti sul NAG.
Al fine di identificare le funzioni proprie del NAG, si fa presente che per i servizi offerti dagli NDOM, il nodo NAG ha il compito di monitorare il livello di servizio rispetto al livello dichiarato dall’Ente, dunque saranno gli stessi NDOM a verificare localmente il proprio operato e soprattutto l’operato degli altri NDOM con i quali cooperano; viceversa, per i servizi offerti dal NAG, devono essere monitorati gli SLA definiti nel Capitolo 6.

Opportuni sistemi di analisi e consultazione di tali dati sono impiegati nel sistema centralizzato di gestione del monitoraggio operativo della qualità dei servizi.

3 Componenti della piattaforma per la realizzazione dei servizi di base per la cooperazione applicativa

Il NAG, che si intende realizzare è un aggregatore di servizi ossia un elemento di intermediazione; esso ha il compito fondamentale di costruire nuovi servizi aggregandone degli altri, ossia dai diversi NDOM.
Le caratteristiche proprie di un NAG che si propone come aggregatore di servizi sono:

- assicurare la fruibilità dei servizi esposti (quindi disponibili) gestendo pubblicazione, ricerca ed accesso ai servizi;
- fornire un ambiente transazionale e sicuro;
- garantire una qualità pre-assegnata dei servizi applicativi (anche quando il servizio è realizzato con la cooperazione di più Enti);
- prevenire o gestire situazioni critiche come attacchi o guasti.

Per il modo in cui è pensato e per le caratteristiche intrinseche che offre, un NAG regionale non deve essere un nodo/ente predominante sugli altri ma piuttosto un nodo appartenente ad una federazione di NAG che appartengono a Enti diversi.
Quanto detto implica che ogni nodo NAG deve essere implementato come un sistema completamente autonomo sia nelle componenti (hardware e software) che nelle funzionalità di aggregazione e controllo della sicurezza, inoltre deve essere tale da poter interagire con una federazione di NAG.
Ogni NAG regionale decide le modalità con cui gli NDOM possono registrarsi, è tuttavia necessario implementare delle strategie opportune per garantire interoperabilità sia tra i vari NDOM che tra i vari NAG; in particolare, le strategie da implementare includono:

- adozione di standard per il formato dei documenti e dei dati trasmessi;
- scelta di metodologie e standard per l’invocazione remota di funzioni disponibili in altri domini applicativi tenendo conto delle problematiche di sicurezza;
- connessione tra i sistemi;
- modalità standard per indicizzare ed interrogare le modalità di accesso ai servizi applicativi ed alle risorse;
- modalità di valutazione dei livelli di servizio dichiarati.

Uno dei requisiti dell’architettura deve essere quello di avere la capacità di adeguarsi alla nascita di nuove necessità, ossia deve garantire la possibilità di ampliare l’insieme dei servizi offerti estendendo il sistema nel suo complesso.
In tale contesto la scalabilità ha una duplice importanza dato che come requisito architetturale deve prevedere la possibilità di includere nell’architettura:

- nuovi Enti che vogliono registrarsi per offrire nuovi servizi,
- altri nodi aggregatori affinché questi possano cooperare nello stesso modo con cui i nodi terminali di vari domini cooperano tra loro.

Occorre realizzare, pertanto, un sistema web-oriented che funga da punto di accesso ai sistemi, ottenendo l’integrazione attraverso l’utilizzo di una interfaccia web omogenea per tutti gli enti e i servizi.

Tale sistema dovrà prevedere l’accesso in sicurezza a:

- Web server, per accedere a pagine web già esistenti (statiche o dinamiche) fornendo all’utente finale un meccanismo integrato per l’accesso.

- Web Services, per accedere a servizi offerti da server providers fornendo all’utente finale un meccanismo integrato per l’accesso, mediante protocolli standard come XML, SOAP, UDDI, etc...
- Direttamente ai servizi offerti da un NDOM, mediante le API che consentono l’accesso diretto ad esso ed alle singole funzionalità che esso offre.

In relazione all’architettura da realizzare descritta nei precedenti paragrafi sono individuate sei componenti funzionali che si devono realizzare ed integrare:

1) componenti per l’integrazione e l’interoperabilità,
2) componenti base per la realizzazione di servizi aggregati,
3) componenti per la gestione della sicurezza,
4) componenti per la gestione dell’accesso multicanale,
5) componenti per la tracciabilità,
6) componenti per il monitoraggio della qualità dei servizi.

Le componenti individuate possono essere realizzate con diverse soluzioni architetturali che prevedendo, ove necessario, il ricorso a più sottosistemi opportunamente integrati per rispettare i vincoli di affidabilità, sicurezza e prestazioni.

È importante evidenziare che il sistema dovrà essere opportunamente dimensionato affinché possa, a regime, gestire oltre 250.000 utenti registrati (utenti di Pubbliche Amministrazioni, Enti Privati e cittadini) e oltre 10.000 servizi da pubblicare nei registri.

E’ richiesto come vincolo imprescindibile del progetto che:

- ogni componente realizzato deve poter essere utilizzato anche autonomamente, per cui è necessario fornire l’insieme delle API che consentono l’accesso diretto ad esso ed alle singole funzionalità che esso offre;
- per i componenti per i quali abbia senso è richiesto un accesso anche in termini di web services;
- ogni componente realizzato deve essere indipendente dalla soluzione tecnologica adottata per gli altri componenti in modo da favorire un eventuale sua sostituzione o modifica;
- l’architettura deve essere scalabile e basata su standard aperti.

Di seguito vengono presentate prima le specifiche generali che il sistema deve presentare e successivamente vengono descritte le componenti.

Si fa esplicitamente notare che:

- le funzioni base del Nodo Aggregatore e le funzioni specifiche relative al sistema CUP devono essere realizzate in due architetture fisicamente distinte, che possano essere allocate in due diversi punti di accesso della rete della Regione Campania;

- le componenti o istanze delle componenti che implementano le funzioni base del NAG possono essere utilizzate, in modo totale o parziale, anche per la realizzazione del sistema CUP, laddove la Ditta fornitrice lo ritenga necessario per la realizzazione dell’applicazione.

3.1 Standard Aperti

Le tecnologie di tutti i componenti che permettono la semplificazione dei problemi di cooperazione e su cui si basano i servizi Web, devono fare riferimento a standard aperti, tra questi, citiamo:

- XML (Extensible Markup Language), un linguaggio di programmazione basato su markup, mediante il quale è possibile descrivere, in maniera gerarchica e formale, la struttura dei dati che vengono inseriti nei documenti XML. In un documento XML i dati vengono immagazzinati in delle unità di memorizzazione, detti elementi XML, che possono essere innestati per realizzare delle strutture dati complesse.

- SOAP (Simple Object Access Protocol), uno standard che descrive, in modo formale, la struttura che devono seguire i documenti XML che rappresentano i messaggi, utilizzati nello scambio di dati tra le entità distribuite, rappresentanti gli elementi architetturali di un Web Service.

- UDDI (Universal Description, Discovery, and Integration) ed ebXML (electronic business XML), due standard di progettazione per gli XML-Registry, che sono dei registri ideati per l’immagazzinamento di tutte le informazioni riguardanti i Web services. A questi registri possono accedere sia le imprese che esportano servizi, per pubblicizzarli, sia i potenziali utenti, per ricercare i servizi necessari.

- WSDL (Web Services Description Language), uno standard che descrive, in maniera formale, come deve essere strutturato un documento XML di descrizione del servizio. Questi documenti descrivono i Web services in maniera particolareggiata, indicando le modalità per accedere al servizio, le funzionalità da questo esportate e la sua locazione fisica. I documenti WSDL possono essere immagazzinati in un XML Registry ed acquisiti dai potenziali clienti per apprendere, in modo automatico, la modalità di accesso al servizio.

Detto ciò, si possono definire “i Web services come componenti Software, descritti mediante dei documenti formali, conformi allo standard WSDL, a cui si può accedere mediante dei protocolli di rete standardizzati, come SOAP su HTTP (HyperText Transfer Protocol)”. Le tecnologie menzionate sono la base delle caratteristiche di maggior interesse per l’uso e lo sviluppo dei Web services, vale a dire interoperabilità ed eterogeneità.

3.2 Specifiche generali per l’integrazione e la pubblicazione

Prima di analizzare nel dettaglio i componenti relativi ai servizi base del NAG, elenchiamo di seguito un insieme di specifiche generali che devono esser soddisfatte da questi componenti.

3.2.1 Specifiche sulle modalità di registrazione dei servizi

Per implementare un sistema basato sulla pubblicazione dei servizi in registri si è deciso di adottare lo standard UDDI. In tal caso per le assunzioni fatte sull’architettura, il registro deve contenere due tipologie di informazioni:

- indirizzo di un servizio,
- indirizzo di un servizio che “punta” ad altri servizi.

Grazie a questo modello scalabile è possibile preservare e rispettare le autonomie dei sistemi preesistenti. In altri termini, l’architettura può facilmente essere vista come nodo unico e “inscriversi” in un’architettura più grande (di livello più alto) nello stesso modo in cui un nodo erogatore si inscrive in un nodo aggregatore (Architettura federata definita nel modello SPICCA).

Tale tipo di organizzazione deve essere realizzata prevedendo la gestione federata dei server registry. Nel rispetto dello standard UDDI, due possibili scenari implementativi devono essere previsti:

- I nodi aggregatori di livello alto registrano i servizi dei nodi aggregatori dei livelli inferiori o dello stesso livello;
- Il registro risultante può essere sia l’unione di tutti i registri che essere strutturato in maniera opportuna in base ai domini (gerarchia di nodi aggregatori) gestendo in maniera distribuita le strategie di sicurezza.

Il soddisfacimento di tali specifiche permetterà ad un registro regionale di essere, eventualmente, “puntato” da un registro Nazionale al fine di realizzare una federazione Nazionale di registri.

Per implementare tali scenari, e dunque offrire servizi cooperativi a valore aggiunto, è necessario garantire l’interoperabilità di tutti i server registry presenti nella piattaforma, nel rispetto dello standard UDDI.

3.2.2 Specifiche sull’accesso

Il processo di accesso è caratterizzato dai fattori di seguito elencati e che devono essere tenuti in conto nella realizzazione del progetto, ed in particolare nella realizzazione dei moduli coinvolti nelle operazioni che gestiscono sessioni di lavoro e transazioni in termini di servizi, contenuti ed accesso alle risorse, sia del nodo aggregatore che dei domini periferici del sistema.
I fattori che determinano lo stato di una sessione di accesso al sistema e la sua evoluzione sono:

- canale di connessione utilizzato (wired, wireless, intranet, extranet, internet)
- protocollo di comunicazione (http, https, ssl, soap, ….)
- terminale client utilizzato (postazione utente, PDA, mobile, …)
- credenziali di accesso accreditate
- metodo di autenticazione (assente, debole, forte, SSO, …)
- modello di cooperazione tra i soggetti partecipanti alla sessione (accesso diretto, accesso a servizio esportato, accesso per delega, …)
- natura dei soggetti comunicanti (utente umano, applicazioni, servizi)
- livello di sicurezza richiesto alla sessione.

3.2.3 Specifiche sulla comunicazione

Ogni sessione di accesso al sistema deve poter essere caratterizzata, disciplinata e gestibile in funzione del canale di comunicazione utilizzato. In particolare, dato che si richiede forte integrazione con il sistema di infrastruttura pre-esistente della Regione Campania, devono poter essere classificate e tracciate le seguenti modalità di accesso:

- Internet

- Extranet
- Intranet

Il canale di connessione deve poter essere identificato dal sistema che gestisce la sicurezza, dai moduli preposti all’autorizzazione, e qualora richiesto da servizi/risorse, questo al fine di poter definire diverse politiche di controllo degli accessi e di erogazione dei servizi, in funzione del canale di comunicazione adottato.
Per le stesse ragioni deve poter distinguere sessioni che avvengono su canale:

- wired
- wireless

Nel caso di connessioni che utilizzino canali misti, la sessione va disciplinata sul canale dotato di specifiche più restrittive in termini di autorizzazioni.

3.2.4 Specifiche di integrazione ed erogazione dei contenuti Web

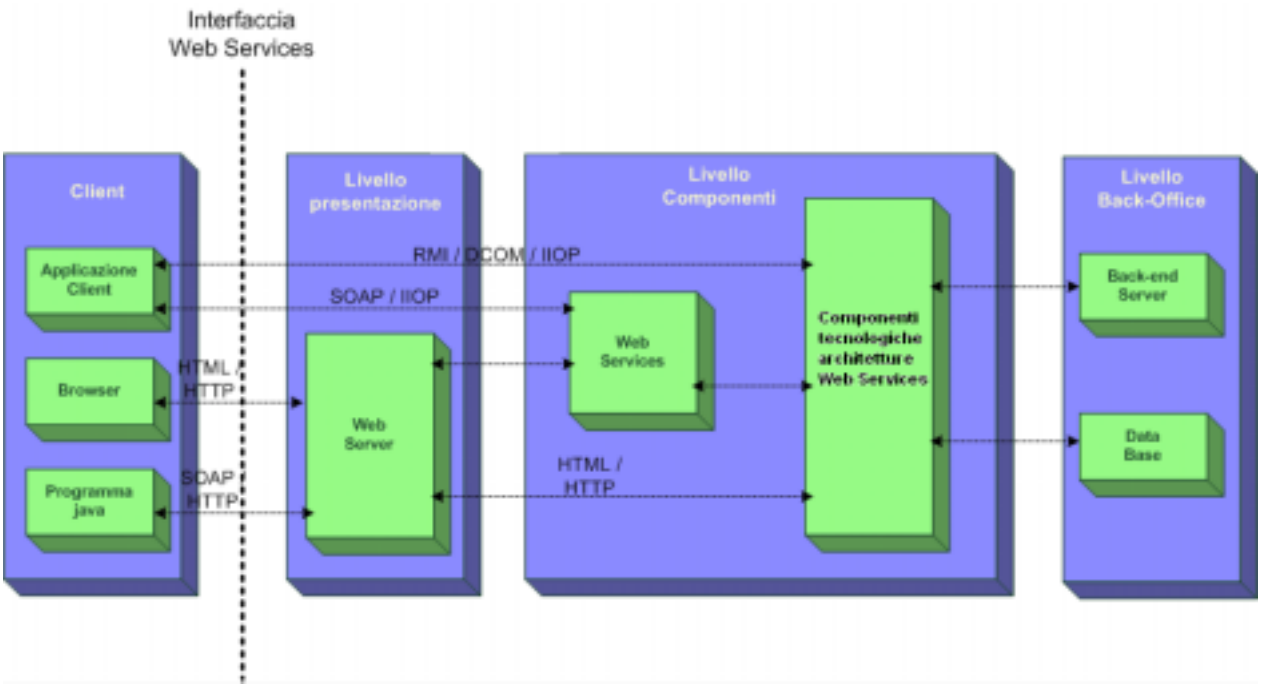
L’integrazione di un server Web esistente può avvenire:

- tramite collegamento ipertestuale: in tal caso il sistema deve unicamente esporre un link del sito web da integrare, rimandando a questi totalmente la gestione dei contenuti
- unificando i contenuti sul sistema: in tal caso è il sistema che espone in maniera diretta i contenuti presenti su altri siti operando periodicamente procedure di allineamento dei dati (Content Management System).

3.2.5 Specifiche di integrazione ed erogazione dei Servizi

L’erogazione dei servizi web va intesa nell’ottica dei Web Services (WS) e quindi il NAG, deve fornire funzionalità di integrazione dei Servizi Web ricorrendo ad un framework di integrazione.

Nella figura seguente viene esposta l’architettura a livelli di riferimento per i Web Services, dove sono riportate le attuali possibili alternative in termini di protocolli, non sono state indicate volutamente le tecnologie base per architetture Web Services al fine di non vincolare la realizzazione del progetto a prodotti di mercato.
Le scelta di standard di riferimento da adottare nel progetto sono state precedentemente esposte (HTTP come protocollo di trasporto e SOAP come protocollo di messaging)



3.3 Componenti per l’integrazione e l’interoperabilità

Il sistema per la gestione dell’integrazione di servizi erogati da enti diversi deve consentire:

- La pubblicazione dei servizi;
- La Ricerca dei servizi;
- La gestione della registrazione di nuovi servizi;
- La realizzazione di servizi aggregati;
- La gestione della busta di e-government.

3.3.1 Pubblicazione dei servizi

La funzione di pubblicazione permette ai fornitori di servizi di renderli visibili ed usufruibili da altri utenti e/o servizi, inoltre permette agli utenti la possibilità di scoprire nuove offerte. In questa sede si intende con il termine generico di “servizio”, un’applicazione utilizzabile anche da client in maniera automatica, e non esclusivamente da utenti umani, ovvero un registro, compatibilmente con le specifiche definite nei sistemi standard, deve contenere due tipologie di informazioni: indirizzo di un servizio e indirizzo di un servizio che punta ad altri servizi.

Tale specifica determina la necessità di realizzare un servizio di pubblicazione che abbia come valore aggiunto alcuni meccanismi in grado di garantire l’usabilità del servizio. Con la pubblicazione occorre quindi garantire:

- Interoperabilità dei servizi,
- Definizione dell’ontologia dei servizi
- Controllo di conformità

L'interoperabilità è una caratteristica che viene garantita scegliendo dei protocolli e formati dei dati per l'interazione tra le diverse applicazioni, e tra le applicazioni e il sistema di gestione, che siano il più possibile indipendenti dalle scelte tecnologiche fatte da ogni ente per la realizzazione del servizio stesso.

L'interoperabilità deve permettere anche l'integrazione tra sistemi automatici diversi, favorendo meccanismi di supporto alla gestione della correttezza dell'interazione. Un sistema automatico, pur avendo gli strumenti per invocare un servizio deve poterlo fare in maniera corretta. Occorre definire quindi, per ogni classe di servizi *un'ontologia* che ne descrive la semantica. Ciò significa che ogni funzionalità del servizio deve essere univocamente identificabile. Tutto ciò deve essere formalizzato definendo un'interfaccia standard per la specifica tipologia di servizi, il formato dei dati ed il processo elaborativo.

Si intende per *conformità* il rispetto, da parte della realizzazione del servizio, sviluppata da un particolare ente, delle specifiche richieste per un suo corretto utilizzo. Nella pratica si deve prevedere una conformità di tipo sintattico analizzando l'interfaccia del servizio ed il corretto funzionamento testando a run time l'applicazione.

3.3.2 Ricerca di un servizio

La funzione di ricerca deve consentire, secondo diversi criteri di selezione, di individuare un servizio o un Ente erogatore di servizi specifici.
Per quanto riguarda le funzioni di ricerca avanzata, deve essere possibile, una volta identificato il richiedente, offrire per tutta la sessione di lavoro un servizio di personalizzazione ed adattamento dei servizi richiesti alle esigenze ed al profilo-terminale utente selezionando:

- Il formato dei dati per l'interfaccia utilizzata lato cliente;
- Il software da scaricare sul terminale utente nel caso in cui sia possibile la riconfigurazione;
- La versione del servizio che è meglio utilizzabile con la migliore qualità.

3.3.3 Gestione della registrazione di servizi

Le operazioni di pubblicazione e di controllo e definizione dei meccanismi di sicurezza vengono eseguite da un componente logico detto ***Autorità di registrazione dei servizi*.**
Il componente di ***Autorità di registrazione dei servizi*** deve operare sia in modo centralizzato, che distribuito.
Quando il fornitore richiede la pubblicazione del servizio, la ***Autorità di registrazione dei servizi*** controlla che il documento che descrive le interfacce del servizio stesso sia conforme alla classe di appartenenza del servizio e che sia dichiarato il livello di servizio offerto che deve essere indirettamente monitorato. Se, invece, si sta aggiungendo un servizio proprio del NAG, la ***Autorità di registrazione dei servizi*** controlla che siano rispettati gli SLA (service level agreement) richiesti; in particolare, l'autorità può eliminare un servizio in caso gli SLA non vengano rispettati.
Nel caso in cui si tratti di una nuova tipologia di servizio occorrerà definire un nuovo formato. Tale operazione non può essere fatta automaticamente e soprattutto il formato verrà definito volta per volta in relazione alla particolare tipologia di servizio.
La ***Autorità di registrazione dei servizi*** si deve occupare anche di implementare le strategie di sicurezza occupandosi di aspetti legati alla:

- gestione delle policy (aggiornamento);
- gestione di nuovi utenti;

- gestione di differenti meccanismi di autenticazione per uno stesso servizio;
- gestione di differenti meccanismi di sicurezza tra domini diversi;
- tracciabilità e monitoraggio.

3.3.4 Componenti base del NAG per la realizzazione di servizi aggregati

Il NAG deve essere realizzato per gestire l’accesso a qualsiasi servizio che può avvenire sia da altre applicazioni software che da utenti che si possono connettere con diversi dispostivi. Esistono pertanto due problematiche di presentazione:

- impiego di meccanismi software che, usando modalità di accesso e rappresentazione del formato dati, consentano ad altre applicazioni software di collegarsi automaticamente ai servizi basandosi su tecnologie ampiamente sviluppate in letteratura;

- realizzazione di sistemi per l’accesso da terminali eterogenei.

In particolare dal NAG deve essere possibile l’accesso in sicurezza a:

- Web server, per accedere a pagine web già esistenti (statiche o dinamiche) fornendo all’utente finale un meccanismo integrato per l’accesso.
- Web Services, per accedere a servizi offerti da server providers fornendo all’utente finale un meccanismo integrato per l’accesso, mediante protocolli standard come XML, SOAP, UDDI, etc...

Esso rappresenta uno strato di intermediazione tra le richieste di utenti o servizi verso i servizi residenti sui sistemi informativi degli Enti stessi; l’intermediatore deve implementare delle opportune strategie di gestione per il rispetto di vincoli tecnologici, ovvero deve essere in grado di implementare correttamente il modello cooperativo definito tra i vari soggetti per la gestione dei servizi (sia esso di tipo Service Oriented Architecture - SOA – o Event Driven Architecture - EDA) e di vincoli organizzativi nel rispetto di norme per la sicurezza, per la privacy, e delle altre esigenze degli Enti coinvolti.
Il componente base richiede la realizzazione di un nucleo software base che fornisca le funzionalità viste nel capitolo precedente; esso deve essere in grado di interagire con i sistemi terminali di accesso (sia utenti esterni che altri servizi) e devono offrire tutti quei servizi che permettono di accedere alla piattaforma rendendo trasparente la modalità di cooperazione tra i servizi che viene adottata ai livelli inferiori (sia EDA che SOA).

Tutti i servizi devono essere erogati garantendo la correttezza delle transazioni effettuate, dove la transazione è intesa come sequenza di operazioni da eseguire in modo atomico. Il mancato completamento di una transazione deve essere supportato da processi di roll-back che devono annullare tutti i cambiamenti effettuati dalla transazione abortita, e riportare lo stato del sistema nelle identiche condizioni di partenza.

Il NAG dunque garantisce e ottimizza l’accesso ai diversi nodi erogatori di servizio operanti nella rete. Il sistema può essere fisicamente costituito da un certo numero di Enti distribuiti geograficamente, i cui servizi sono accessibili attraverso un punto di accesso esterno per gli utenti esterni o per altri NAG; oppure da punti interni (quando un servizio richiede la cooperazione di un altro servizio appartenente allo stesso NAG) sempre mediante il NAG che funge da intermediatore implementando anche gli opportuni meccanismi di autenticazione.

Notiamo esplicitamente che la fornitura deve includere la documentazione relativa a tutte le modalità di accesso possibili sia ai singoli componenti che alle specifiche funzionalità e deve includere la documentazione relativa alle modalità di configurazione delle stesse.

Il sistema di gestione deve essere in grado di aggregare più servizi quando si rende necessaria una loro integrazione per offrire all'utente il risultato finale della sua interrogazione.

Per la realizzazione delle funzionalità di interoperabilità, il NAG deve essere dotato di ulteriori componenti che possono essere utilizzate anche in modo non integrato:

- Servizi di file sharing,
- Servizi di Web Hosting,
- Servizi di Web caching e Proxy,
- Sevizi di Content Management,
- DataBase Server,
- Servizi di WorkFlow di supporto alla gestione dei servizi offerti dal NAG,

3.3.5 Componenti per la gestione della busta di E-government

Il sistema deve essere in grado di gestire applicazioni basate sull'impiego della busta di e-government, così come definito dalla Presidenza del Consiglio dei Ministri in relazione ai progetti di e-government nazionali.
In particolare deve essere realizzato un modulo che consenta sia in ricezione che in trasmissione di effettuare tutti i controlli sulla corretta formazione della busta e di smistare la busta all'Ente di dominio (NDOM) destinatario. Tutto il processo deve ovviamente essere tracciato e monitorato in relazione a quanto definito nei paragrafi precedenti. Ad esempio, va monitorato l'evento di ricezione e di trasmissione della busta da e verso un dominio.

3.4 Componenti per la gestione della sicurezza

3.4.1 Introduzione

Il nodo Aggregatore, ed in particolare le componenti preposte alla sicurezza, devono garantire i seguenti requisiti, sia per i contenuti Web che per i servizi erogati via Web Services:

- Riservatezza: Salvaguardare le privacy delle informazioni e l'accesso alle stesse quando privi di autorizzazione, sia nel caso in cui esse risultino archiviate su un supporto fisico, che in transito sui sistemi.
- Integrità: Assicurare che dati critici non vengano alterati in modo malizioso o involontariamente, sia nel caso in cui esse risultino archiviate su un supporto fisico, che nel corso di una transazione.
- Accountability: Rilevare, tracciare e documentare le attività di accesso e di sessione di ogni singolo utente; garantire il non ripudio della paternità di una azione intrapresa; prevedere attività di logging di tutti gli eventi che si verificano dall'accesso ai servizi all'uscita dal sistema.

- Monitoraggio sicurezza ed Auditing: Insieme di attività di sorveglianza e monitoraggio atte a rilevare intrusioni, attacchi e minacce verso il sistema e le sue componenti. Processi periodici di valutazione dell’effettivo livello di sicurezza del sistema. Analisi di possibili vulnerabilità insorte o indotte.

I componenti per la gestione della sicurezza devono tenere in considerazione alcuni aspetti fondamentali quali:

1) tenere in considerazione le specifiche peculiarità sia dei nodi (NAG ed NDOM) che dei terminali eterogenei che possono accedere alla piattaforma;
2) implementare meccanismi di autenticazione ed autorizzazione “forti” e “deboli”;
3) gestire in maniera integrata il controllo degli accessi a tutte le risorse del sistema garantendo l’applicazione di policy di accesso sia di tipo generale estese all’intero sistema, che di policy locali gestite autonomamente dai singoli NDOM.
4) implementare la sicurezza per i Web Services, per i server web e per tutti i componenti del sistema.

In particolare, il primo punto evidenzia il fatto che i componenti per la sicurezza devono essere pensati in funzione della multicanalità, ovvero esistono terminali eterogenei da cui si può accedere al sistema ed è necessario prevedere opportuni meccanismi di autenticazione ed autorizzazione supportabili da tali tipologie di terminali.
Il secondo punto evidenzia la necessità di prevedere differenti livelli di autenticazione ed autorizzazione che siano funzione dei possibili ruoli che un soggetto può assumere all’interno di ogni singolo Ente o di servizi che richiedono l’accesso ad altri servizi.
Nei prossimi paragrafi verrà illustrata l’architettura di sicurezza in grado di mettere in opera sia la gestione di differenti livelli di autenticazione che di autorizzazione; in particolare, per quanto riguarda l’autenticazione devono essere previsti almeno i seguenti livelli:

- meccanismi deboli:
  - autenticazione con login e password,
  - autenticazione con password di tipo sfida/risposta crittata;
- meccanismi forti:
  - Certificato digitale su dispositivo fisico;
  - Certificato digitale su Smart Card;
  - Certificato digitale su supporti compatibili con la carta di identità elettronica, o una carta servizi.
  - Autenticazione tramite dispositivi biometrici.

Per quanto riguarda i meccanismi di autorizzazione devono essere previste differenti modalità a seconda di dove e come si prendono le credenziali di un utente; i meccanismi previsti devono includere almeno le seguenti modalità:

- prelevamento delle credenziali da un server gestito localmente sui nodi NDOM o centralmente sul nodo NAG;
- prelevamento delle credenziali da un certificato di identità predisposto per l’attribuzione del ruolo nel campo subject;
- prelevamento delle credenziali da un certificato di attributo.

L’associazione delle credenziali di un utente alle specifiche funzionalità e risorse a cui ha accesso all’interno del sistema, è gestita mediante l’uso di politiche (policy) per il controllo degli accessi e sistemi per la gestione e la valutazione di tali policy.

I servizi di sicurezza del sistema informatico devono includere:

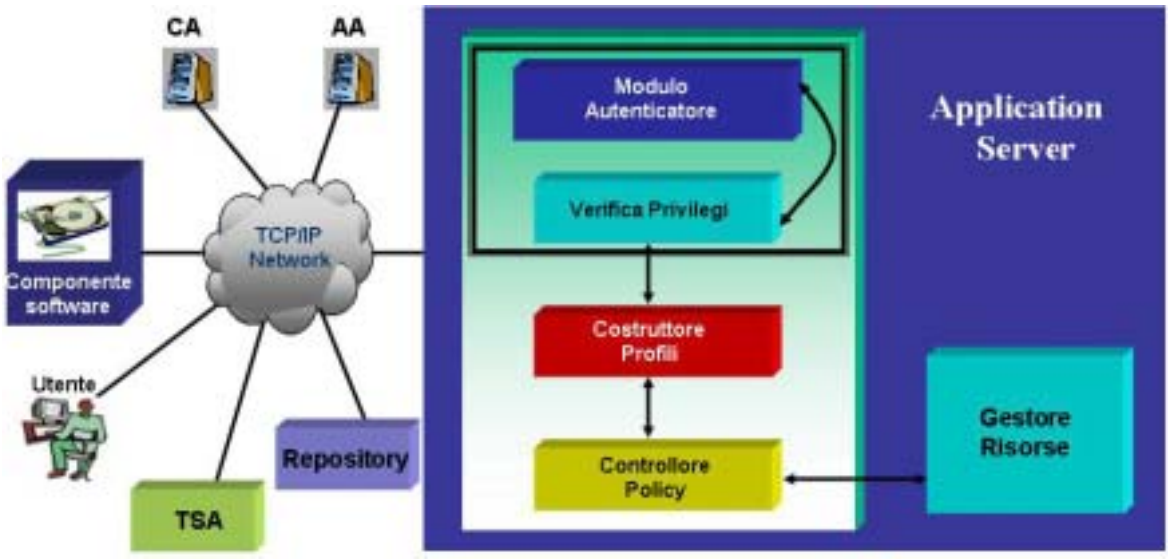
- Controllo degli accessi,
- Servizi di Certificazione e Pubblicazione dei certificati,
- Monitoraggio ed Auditing.

I dettagli dei componenti sono illustrati di seguito mentre dei possibili scenari d’uso verranno successivamente illustrati in un altro Capitolo, al fine di esemplificare alcune condizioni operative del sistema

3.4.2 Modello di riferimento per il controllo degli accessi

Il modello concettuale di questo componente è riportato nella figura seguente. Per quanto riguarda le tecnologie, non viene fatta alcuna scelta proprietaria. Al contrario, si sottolinea la necessità di ricorrere a soluzioni “vendor neutral” e conformi ai principali standard internazionali per sistemi aperti.

La figura non riporta esplicitamente i componenti responsabili delle attività di monitoraggio ed auditing, che sono comunque da considerarsi trasversali (occorrerà cioè prevedere lo svolgimento di tali attività all’interno di tutti i componenti dell’architettura e dell’infrastruttura di comunicazione).



Modello concettuale di un generico sevizio operante in sicurezza

Nel disegno si è indicato con CA l’autorità di certificazione, con AA l’autorità per la gestione degli attributi (ruoli) legati ad un utente o un servizio certificati dalla CA e con TSA un autorità per la gestione del tempo.
Osserviamo esplicitamente che le diverse autorità esplicano le loro funzioni limitatamente al dominio di appartenenza degli utenti ed è interesse della Regione Campania realizzare una Infrastruttura a Chiave Pubblica per la Firma elettronica ad uso interno e non per la Firma Digitale a validità giuridica.

I certificati digitali emessi dalla CA saranno utilizzati in differenti contesti,ad esempio nel processo di autenticazione mediante Certificati di identità o nel protocollo di sfida e risposta; per firmare dati, documenti e/o messaggi XML; per realizzare protocolli sicuri, etc….
E’ importante notare che la piattaforma non deve subire degradazioni in termini funzionali se la Regione Campania dovesse decidere di utilizzare una Infrastruttura a Chiave Pubblica a validità giuridica.
Il Controllo degli accessi ha come obiettivo la realizzazione e la gestione di un sistema di profilatura avanzata di utenti e sistemi, all’interno di un contesto operativo vario nelle strutture e nelle dinamiche.
A tale risultato si perviene applicando strategie di identificazione dei soggetti e dei ruoli, ben configurabili ed adattabili al contesto.
La gestione dei ruoli si basa su una politica di controllo di tipo RBAC (Role Based Access Control). Questa politica è stata scelta per le sue caratteristiche di flessibilità e manutenibilità. La nozione di base su cui si fonda tale metodologia è il concetto di *ruolo*: il ruolo può essere definito come un sottoinsieme dei permessi necessari per accedere a tutto il sistema. Ogni soggetto può assumere uno o più ruoli durante una transazione ottenendo i relativi permessi di accesso. In altre parole i permessi sono associati ad un ruolo ed ad ogni utente è associato uno o più ruoli.

I Servizi di certificazione e pubblicazione su directory delle credenziali, costituiscono gli strumenti base comune, grazie a quali è possibile implementare il c*ontrollo degli accessi*.
La certificazione delle identità dei soggetti, siano essi persone o componenti del sistema, e la chiara definizione dei loro ruoli, sono servizi che devono essere garantiti e supportati dall’intera infrastruttura; devono dunque essere previste delle Registration Authority distribuite sul territorio ma collegate in sicurezza alle CA e AA di riferimento.
A tale tipo di certificazione si affianca il servizio di certificazione temporale, il cui compito è fornire precisi riferimenti cronologici su transazioni effettuate, tracciabilità di flussi procedurali, e firme temporali. La facile reperibilità e l’accesso ad informazioni relative alle identità dei soggetti, ai loro rispettivi ruoli, ed alle marche temporali utilizzate nella certificazione del tempo, devono essere garantiti da adeguati servizi di directory per la pubblicazione.

Nella figura viene riportata la struttura per la definizione degli utenti e dei loro privilegi, ed i componenti responsabili delle varie attività. Nell'architettura troviamo tre componenti principali:

- *Modulo di autenticazione*: implementa l'algoritmo di autenticazione garantendo l'identità dell'utente;
- *Verificatore di Privilegi*: garantisce che l'utente possa rivestire solo ruoli a lui autorizzati;
- *Costruttore di Profili*: genera dinamicamente il profilo dell’utente in base alle credenziali presentate;
- *Controllore di Policy*: assicura che gli accessi siano concessi solo a soggetti aventi i ruoli appropriati.

Nell'architettura viene riportato anche il componente software che interagisce con tutti gli altri componenti dell'architettura e precisamente:

- utilizza certificati a chiave pubblica;
- utilizza certificati d'attributo;
- interagisce con il Modulo di Autenticazione per autenticarsi;
- interagisce con il Verificatore di privilegi per rivestire un ruolo;
- effettua richieste HTTP gestite dal resource manager e filtrate dal Controllore di Policy.

Ad ogni sessione, al soggetto è associata una Active Role List (ARL) che definisce i ruoli correntemente rivestiti dal soggetto stesso. Per assumere un determinato ruolo l'utente interagisce con il Verificatore di privilegi.

L’efficacia di tale infrastruttura di sicurezza è fortemente condizionata dalla corretta interpretazione dell’oggetto su cui si vuole intervenire, e dagli obiettivi di protezione che si intendono perseguire.
Il sistema, o l’insieme di sistemi intesi come un’organizzazione, da porre in sicurezza, va sottoposto a procedure di analisi finalizzate ad individuare sia gli asset da proteggere che il livello di criticità degli stessi.
La chiara definizione dei livelli di rischio associati ad ogni asset analizzato, viene tradotta in opportuni livelli di sicurezza desiderati per ogni singolo asset.
I risultati di tale analisi forniscono la base su cui poter sviluppare efficaci policy di sicurezza.
L’implementazione di una determinata policy, è realizzata applicando il Controllo degli accessi che a sua volta utilizza i servizi di certificazione come strumenti.
Tutti i servizi ed i controlli, vanno ben progettati e differenziati a valle di procedure di auditing condotte preliminarmente sull’organizzazione e sugli asset di valore strategico e costituiscono elemento fondamentale del documento sul Risk Assesment definito nel Capitolo 6.

3.4.3 Specifiche per la sicurezza

3.4.3.1 Specifiche sui meccanismi di accesso

Tutti i servizi devono poter essere accessibili dalla piattaforma attraverso i meccanismi di sicurezza che devono sottoporre gli utenti ad Autenticazione e ad Autorizzazione. Solo in questo modo sono gestibili le esigenze di Riservatezza, Integrità, Tracciabilità e Disponibilità richieste al sistema.

Autenticazione:
L’Autenticazione deve essere contemplata da tutte le risorse ed i servizi erogati dal sistema.
E’ necessario prevedere quattro modalità di autenticazione:

- autenticazione assente
- autenticazione locale sui nodi erogatori;
- autenticazione centralizzata sul nodo aggregatore.
- autenticazione mista sia locale che sul nodo aggregatore.

Autorizzazione:

Ogni soggetto può assumere uno o più ruoli durante una transazione ottenendo i relativi permessi di accesso in funzione delle credenziali di ruolo possedute o presentate.
In altre parole i permessi sono associati ad un ruolo ed ad ogni utente è associato uno o più ruoli.

A tale modello viene aggiunto un sistema alternativo di autorizzazione, basato unicamente sull’identità dell’utente e sulla facoltà del servizio/risorsa di poter concedere autorizzazioni in funzione della sola autenticazione, naturalmente ciò è possibile se al servizio/risorsa può usufruire di un repository di profili di autorizzazione per ogni utente registrato.

Il cartesiano dei due modelli di Autorizzazione, genera quattro possibili scenari che possono a loro volta essere applicabili su ognuno dei quattro schemi di Autenticazione visti in precedenza.

I modelli di Autorizzazione sono dunque:

- Autorizzazione non richiesta
- Autorizzazione sull’utente
- Autorizzazione sul ruolo
- Autorizzazione come risultante di utente + ruolo

Tali modalità possono coesistere all’interno della stessa infrastruttura e quindi essere adottate nella stessa transazione, in quanto la transazione può coinvolgere domini diversi, ove diverse risultano le politiche di autenticazione e di autorizzazione.

Il progetto deve poter garantire la possibilità di contemplare tutti i modelli di Autenticazione ed Autorizzazione esposti.

Anche se tutti gli scenari esposti ricalcano una tassonomia delle possibili modalità di accesso condizionato all’autenticazione-autorizzazione che il sistema deve contemplare, il modello di riferimento cui ci si dovrebbe attenere in modo preferenziale, in particolar modo per tutte le nuove implementazione dei nuovi servizi Web Services, è quello che viene denominato *Modello integrato* ed esposto in dettaglio nel seguito nel paragrafo relativo ai Web Services.

Questo modello presuppone la realizzazione di un’infrastruttura di sicurezza trasversale a tutte le componenti del sistema che garantiscono la sicurezza come servizio fornito dal NAG, e richiamabile tramite interfacce standard da tutti i domini. Le interfacce devono essere tali da poter garantire un’unica autenticazione sul NAG, ed attraverso la gestione di un contesto di sicurezza associato ad una sessione di lavoro, si permetta di operare in modo trasparente attraversando domini diversi senza dover reiterare le operazioni di autenticazione-autorizzazione.

Resta comunque valida, la possibilità di poter gestire il controllo degli accessi in modo autonomo laddove venga esplicitamente richiesto o tecnicamente non realizzabile.

I repository di credenziali devono essere sistemi di directory LDAP (Lightweight Directory Access Protocol).

Fornitura Credenziali:

Coerentemente alle politiche di controllo degli accessi che possono variare tra i vari domini, devono poter essere contemplate modalità di fornitura differenti. In particolare sono previsti due modelli di fornitura delle credenziali.

- **Modello integrato**: una volta autenticato è il sistema a gestire la ricerca delle credenziali del soggetto ed a sottoporle ai servizi/risorse che richiedono tali credenziali.
- **Modello autonomo**: quando l’utente accede ad un servizio/risorsa è questo che si fa carico di richiedere e validare le credenziali dell’utente. Autenticazione ed autorizzazione sono entrambe gestite localmente, nel caso la transazione dovesse coinvolgere più domini, le credenziali posso essere richieste da ogni dominio.

Ulteriori dettagli su i due modelli sono riportati in seguito nel paragrafo relativo agli scenari d’uso

3.4.3.2 Specifiche per l'accesso in sicurezza dei contenuti Web

I contenuti web integrati dal sistema devono in funzione della loro criticità essere posti in sicurezza e soggetti anch'essi a procedure di controllo degli accessi.
Le specifiche di sicurezza richieste per il sistema web e per i siti dei domini locali, devono ove richiesto supportare:

- Autenticazione ed Autorizzazione utente.
- Sistemi ed architetture SSO (Single Sign On), ove esplicitamente richiesto e possibile.
- Impiego dei principali protocolli crittografici:
  - SSL
  - TLS
  - HTTPS

3.4.3.3 Specifiche per l'accesso in sicurezza dei Web Services

I servizi erogati dai Web Services devono anch'essi presentare un livello di sicurezza adeguato, indicato nel documento sulle specifiche di sicurezza risultato dei processi di Risk Assessment e Risk Management, che sarà richiesto nello sviluppo del progetto secondo quanto indicato in un successivo capitolo. I singoli servizi erogati, presentano differenti livelli di sicurezza, e dovranno di conseguenza essere messi in protezione da un livello di sicurezza proporzionale alla criticità che li caratterizza.
Solo utenti identificati ed autorizzati devono poter usufruire dei servizi Web Services, a meno che questi vengano erogati in modo pubblico ed indiscriminato.
Anche il semplice accesso alla ricerca dei servizi forniti, ed ai meccanismi di discovery, come ad esempio UDDI, necessitano di essere gestiti da meccanismi di controllo, sia in termini di Autenticazione che di Autorizzazione.
L'obiettivo a cui si deve tendere è quello di creare uno *user security context*, inteso come una combinazione di identità utente e di attributi di sicurezza, che durante una transazione deve attraversare tutti i tier di un architettura Web Services.
Disporre di uno *user security context*, elimina l'esigenza di riautenticare l'utente quando la sua richiesta di servizio passa da un tier all'altro.

Dettaglio specifiche:

- E' necessaria l'adozione di un modello unificato di sicurezza per il progetto della sicurezza dei servizi Web Services e non lasciare che ogni singolo dominio definisca un modello di sicurezza arbitrario; il rispetto dell'autonomia delle policy di gestione locale deve essere comunque garantito.
- Tutti i servizi di sicurezza critici devono essere forniti sull'intero percorso end-to-end di un'architettura multitier tipica di un Web Services.
- Ogni transazione eseguita via Web Services deve essere tracciabile dalla sua origine fino alla sua conclusione, garantendo un livello di sicurezza consistente attraverso i processi che coinvolgono tutti i domini ed i tier dell'architettura.
- Deve essere possibile ove richiesto poter eseguire procedure di auditing e disporre di accurati record delle sequenze di passi necessari a completare una transazione Web Services.
- L'integrazione deve essere applicata anche all'infrastruttura di sicurezza, permettendo alle tecnologie di sicurezza perimetrale, di front end, di middle e di back-office di poter

interoperare, costituendo un unico framework per la sicurezza che si estenda sull’intero percorso end-to-end.
- I Messaggi XML devono poter essere firmati digitalmente e criptati qualora un servizio lo richieda.
- Deve essere supportato un meccanismo basato su XML per lo scambio via rete di informazioni di autenticazione, autorizzazione ed asserzione di attributi tra organizzazioni partner.
- La soluzione proposta deve essere aperta e non vincolata a soluzioni vendor.

3.4.4 Componenti per la sicurezza

Nel quadro precedentemente delineato si descrivono, nello specifico, le componenti per la sicurezza che implementano il modello:
- Componenti per il controllo degli accessi;
- Componenti per il servizio di Directory per Certificati e Credenziali;
- Componenti per la Certificazione di identità e privilegi;
- Componenti per la Certificazione del tempo;
- Componenti per il Monitoraggio e l’ Auditing.

3.4.4.1 Componenti per il Controllo degli accessi

Le principali problematiche che coinvolgono il controllo degli accessi riguardano la rappresentazione della politica di controllo da utilizzare. Questo aspetto è di per sé il più importante ed il più discusso poiché la scelta della politica di controllo degli accessi influisce sulla manutenibilità del sistema e sulla sua efficienza, con particolare riguardo alla capacità del sistema di attuare i criteri di protezione desiderati dall'amministratore della sicurezza.

Il sistema deve essere facilmente configurabile e deve permettere di utilizzare delle policy molto flessibili che tengano conto non solo dei privilegi dell'utente collegato ma anche di parametri aggiuntivi, quali la localizzazione dell'utente, il metodo utilizzato per l'autenticazione. Il sistema deve permettere un controllo degli accessi a grana molto fine in modo da poter negare l'accesso a servizi, a pagine Web o a frammenti di pagina. Questo permette di utilizzare la stessa pagina Web per utenti con privilegi diversi presentando solo le parti della pagina cui è concesso accedere. Ad esempio ad un utente cui non è permesso sfruttare un particolare servizio si deve presentare la stessa pagina presentata all'utente in grado di utilizzare il servizio, ma senza la visibilità dell'opportuno tasto utilizzato per sottoporre al Web server la richiesta per tale servizio. Il sistema di controllo degli accessi deve essere completamente trasparente allo sviluppatore Web, in tal modo l'amministratore della sicurezza non ha la necessità di interagire con gli sviluppatori per attuare una data policy. Ad esempio, sovente quando un utente non ha diritto di accesso ad una pagina deve essere reindirizzato ad una pagina di login; tale operazione è di solito “cablata” nel codice delle pagine Web per cui una modifica a tale politica richiede l'intervento dello sviluppatore. L’intento è quello di fornire mezzi per ovviare a tale inopportuna interazione tra l'amministratore della sicurezza e lo sviluppatore dell'applicazione. L'indipendenza tra il sistema di controllo e l'applicazione consentirà di riapplicare il sistema di controllo ad altre applicazioni con modifiche minime alle stesse.

Per facilitare le mansioni dell'amministratore del sistema è necessario implementare il modello di controllo degli accessi indicato come *Role Based Access Control* (RBAC).

È compito dell’Impresa definire delle policy che siano funzione dei ruoli e delle risorse della piattaforma; tali policy costituiscono parte del Piano della Sicurezza; sarà poi compito degli amministratori della sicurezza scrivere le policy specifiche in funzione dei ruoli specifici ricoperti dagli utenti dei vari Enti e in funzione delle risorse da proteggere.
Per illustrare le varie modalità di funzionamento si rimanda al capitolo sugli scenari applicativi.

3.4.4.2 Componenti per il servizio di Directory per Certificati e Credenziali

I sistemi di pubblicazione delle informazioni relative ai servizi di certificazione, devono essere gestiti da un repository di servizi di directory su server dedicati. Un servizio di directory è un database specializzato ed ottimizzato per l’accesso, la navigazione e la ricerca, soprattutto in archivi strutturati in alberi gerarchici.

Il principale standard di accesso a servizi di directory è il protocollo LDAP (Lightweight Directory Access Protocol) ed è questo lo standard che si vuole adottare.
Tutti i certificati emessi dall’infrastruttura, le liste di revoca (CRL) e le liste di sospensione (CSL) devono essere disponibili e consultabili in modo continuativo attraverso il protocollo LDAP presso un sito comunque controllabile dalla Regione Campania.

3.4.4.3 Componenti per la Certificazione di identità e privilegi

Gli utenti che possono rivestire dei ruoli specifici devono essere registrati presso una Certification Authority (CA) ad uso interno e presso una Attribute Authority (AA) per utilizzare meccanismi di autenticazione deboli o forti.
L'associazione dei ruoli ai singoli utenti è operata in diversi modi:

- prelevamento delle credenziali da un DBserver gestito localmente sui nodi NDOM o centralmente sul nodo NAG;
- prelevamento delle credenziali da un certificato di identità predisposto per l’attribuzione del ruolo nel campo subject;
- prelevamento delle credenziali da un certificato di attributo (AC) per ognuno dei ruoli che l'utente può rivestire.

Si deve prevedere, per motivi sia tecnici che organizzativi, sia l’impiego di un unico AC nel quale siano elencati tutti i ruoli assumibili dall'utente che la possibilità di generare più AC con l’individuazione di ruoli singoli; inoltre è possibile utilizzare anche informazioni estratte dal certificato digitale (campo subject).

La definizione dei permessi associati ad ogni ruolo e dei vincoli aggiuntivi (e dunque della definizione delle politiche di accesso) è demandata all'amministratore della sicurezza.
Per tutti i servizi non sensibili sarà possibile prevedere l’accesso da parte di utenti esterni, anche senza procedure di autenticazione.

3.4.4.4 Componenti per la Certificazione del tempo

Lo scopo di un sistema di certificazione del tempo è di permettere ad un’applicazione software o ad un utente umano di ottenere evidenza informatica dell’esistenza di un dato in un certo istante (Absolute Temporal Authentication) o prima di un altro dato (Relative Temporal Authentication).
La “granularità temporale” della TSA deve poter essere configurata arbitrariamente in funzione dell’applicazione richiedente.
Per le esigenze discusse in precedenza, occorrerà consentire l’uso dei servizi di time stamping senza dover essere a conoscenza delle specifiche di protocollo e di formato che sono utilizzate per l’implementazione del servizio stesso.

Lo scenario architetturale prevede l’implementazione di un’interfaccia tra le applicazioni client ed i server di marcatura temporale, che ha il compito di raccogliere le semplici richieste di servizio dei vari client che ad essa ricorrono, per sottoporle al server di time stamp, non prima però di aver costruito l’idoneo formato della richiesta con cui essa può essere correttamente processata. Una tale architettura deve, quindi, saper parlare da un lato con i client e dall’altro col time stamping server, realizzando il giusto protocollo di trasmissione in accordo con le authority; in definitiva, l’architettura da realizzare deve consentire di rendere completamente oscuro all’utente il tipo di back-end di marcatura temporale.

3.4.4.5 Componenti per il Monitoraggio e l’Auditing

Di seguito si riportano alcune osservazioni specifiche per il controllo della sicurezza fisica della piattaforma che si deve realizzare.
Un buon approccio nell’implementare un’infrastruttura di sicurezza all’interno di un’organizzazione consiste nella corretta valutazione in termini di livello di esposizione al rischio del sistema e delle sue componenti.
Avviare in prima istanza un processo di risk assessment, è il migliore approccio per ottenere una profilatura degli asset critici. Tale processo affidandosi a procedure di auditing permette di inventariare le componenti del sistema (dati, risorse, processi, ecc.) che necessitano di essere poste in sicurezza, di classificarle opportunamente assegnando ad ognuna di esse un livello di criticità in funzione dell’esposizione a minacce ed all’importanza strategica rivestita nel sistema.
I risultati del processo di auditing, sottoposti ad analisi, costituiscono la base di partenza per poter stilare policy di sicurezza efficaci, ed improntare funzioni di controllo opportune a garantire il livello di sicurezza richiesto da ogni singolo asset.

Il mantenimento di un adeguato livello di sicurezza può essere garantito unicamente se è attuata costantemente una politica di monitoraggio sul sistema e sulle sue componenti.
La mancanza di controllo può vanificare la validità dell’intera infrastruttura di sicurezza, se l’evidenza di un danno derivante da un attacco, è palesata solo dopo il suo compimento e non in tempi brevi o auspicabilmente nel momento stesso in cui esso viene perpetrato.

L’insieme di controlli preposti al monitoraggio del sistema, per quanto detto prima, è fortemente condizionato dall’analisi preliminare effettuata nel risk assessment, per questo motivo non è possibile configurare univocamente un sistema di monitoraggio prescindendo dal contesto in cui esso verrà calato. Ciò presupposto deve essere previsto un modello configurabile comprendente le principali tipologie di strumenti di monitoraggio e controllo che va opportunamente tarato e dimensionato in funzione dello scenario applicativo.

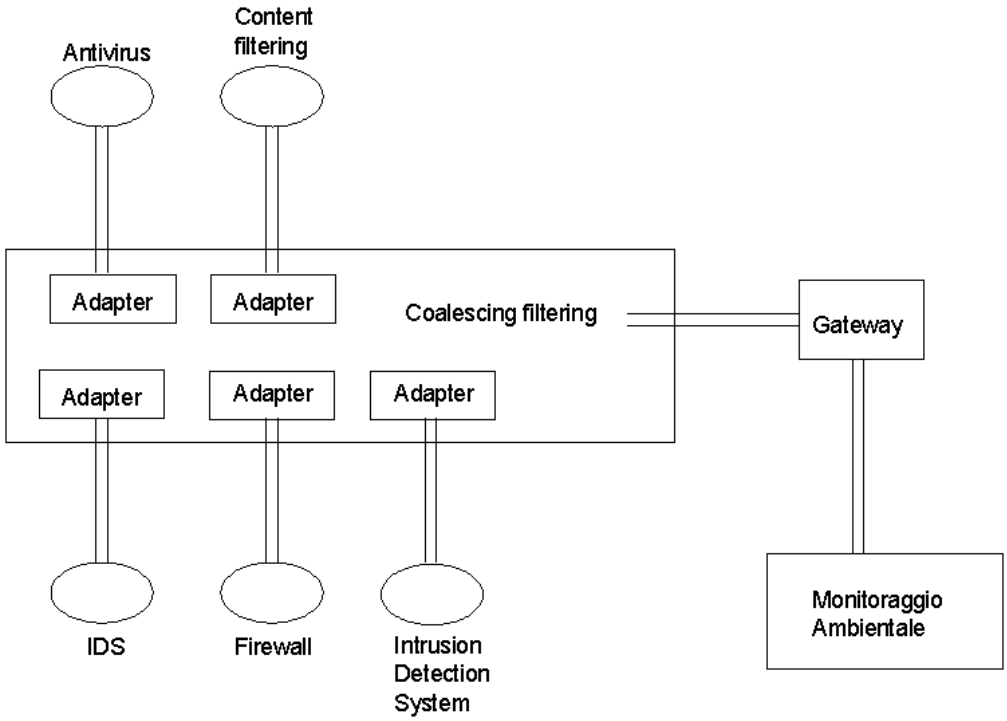
Gli strumenti di monitoraggio e di un’infrastruttura di sicurezza oltre a svolgere mansioni di sorveglianza, devono essere in grado di offrire anche azioni di autodifesa autonome capaci di garantire un primo livello di autodifesa in presenza di attacchi.

In alcuni casi la scelta dei sistemi di monitoraggio e controllo deve essere effettuata tentando di conferire all’infrastruttura di sicurezza un carattere proattivo, anticipando l’insorgere di nuove vulnerabilità, dotandosi sia di apparati capaci di aggiornarsi autonomamente nei confronti delle nuove tipologie di attacco, sia gestendo la manutenzione e l’aggiornamento dei sistemi con operatori umani; caso tipico è l’aggiornamento delle “attack signatures” di un sistema NIDS o dell’archivio dei virus noti.
Le principali tipologie di sistemi di monitoraggio e controllo che devono essere integrate nell’architettura sono:

- Firewall
- NIDS (network intrusion detection system)
- Antivirus - worms
- Content Filtering
- Traffic Shaping
- Antispam

Un sistema integrato per la sicurezza di un sistema eterogeneo, deve poter gestire in modo centralizzato tutti i segnali provenienti dai sensori e dai sistemi di monitoraggio.
Il monitoraggio è efficace quando garantisce un’attività di supervisione costante e globale. Opportuni sensori e detector collocati in più punti del sistema, devono essere capaci di generare, in presenza di eventi anomali, segnali di alert, che in prima istanza possano essere processati da sistemi automatici capaci di attivare in tempi brevi procedure di recovery, di alzare il livello di guardia attivando ulteriori sensori, fino all’attivazione di sistemi di monitoraggio ambientale.
Questo ha senso se la gestione di tali segnali è centralizzata.

Il management centralizzato è realizzato aggregando il flusso di informazioni proveniente dai sensori dei terminali di controllo, su di un canale di comunicazione comune che segnala ogni alert ad un unico gateway preposto al ruolo di componente intelligente capace di svolgere mansioni di coalescing filtering, log analisys, soppressione di falsi positivi, e qualora vengano rilevate condizioni di allerta critiche, l’avvio di particolari procedure difensive che vanno dall’innalzamento dei livelli di soglia di allerta, alla generazione di segnali di alto livello (allarmi ambientali, e-mail, telefonate, sms), fino all’attivazione di sistemi di monitoraggio ambientale.
Per poter comunicare con il bus centrale i vari sensori e controlli periferici si interfacciano con il canale di coalescing filtering attraverso particolari adapter che svolgono il ruolo di traduttore, interpretando ed uniformando i diversi segnali provenienti dai vari dispositivi in un unico standard supportato dal gateway che gestisce il canale.
A scopo esemplificativo, è riportata in figura una possibile struttura logica per l’integrazione di sistemi di monitoraggio e di controllo:



Modello integrato di sistemi di sicurezza per il monitoraggio ed il controllo.

L'analisi dei dati derivanti dall'esecuzione periodica di audit, dai log dell'attività di monitoraggio e dai report di eventuali incidenti, costituiscono il feedback necessario su cui avviare ciclicamente procedure di analisi volte a rivalutare il sistema.
A valle di tale analisi, qualora si renda necessario, bisogna procedere alla rimodulazione delle policy di sicurezza oppure, in presenza di radicali mutamenti del contesto, all'elaborazione di nuove.

3.5 Componenti per la gestione dell'accesso multicanale

La piattaforma dovrà supportare l'eterogeneità delle diverse tecnologie di rete e dei diversi dispositivi client attualmente disponibili ed abbondantemente utilizzate.
Data la eterogeneità dei canali e dei protocolli di accesso, è necessario prevedere dei servizi che si occupino della gestione delle diverse tecnologie di rete in maniera del tutto trasparente all'utente.
I servizi devono prevedere sia le modalità di accesso di tipo tradizionale (accesso ad internet, portali web, e-commerce,…) che quelle di nuova generazione (UMTS, reti satellitari,…), tali servizi agiscono in stretta collaborazione con i servizi di presentazione.

Per l'accesso multicanale, la necessità di dover gestire terminali eterogenei, richiede la disponibilità del seguente set minimale di protocolli di accesso:

- WAP
- HTTP
- HTTPS
- SOAP

Per ogni protocollo utilizzato deve essere possibile l'accesso differenziato ai servizi disponibili nel sistema.

In particolare il componente di personalizzazione dell’accesso deve essere in grado di riconoscere i profili terminale descritti secondo gli standard più diffusi quali CC/PP (Composite Capabilities/Preferences Profile) per poter offrire i servizi nella forma più adatta alle capability dei dispositivi.
Tale modulo dovrà interfacciarsi con il sistema di autenticazione ed autorizzazione selezionando in base al particolare terminale anche i meccanismi di autenticazione supportati.
Identificato l’utente tale modulo dovrà offrire per tutta la sessione di lavoro un servizio di personalizzazione ed adattamento dei servizi richiesti alle esigenze ed al profilo-terminale utente selezionando:

- Il formato dei dati per l’interfaccia utilizzata lato cliente
- Il software da scaricare sul terminale utente nel caso in cui sia possibile la riconfigurazione
- La versione del servizio che è meglio utilizzabile con la migliore qualità apprezzabile

Dovendo garantire la funzionalità di aggregazione e di supporto dell’eterogeneità è necessario che il sistema utilizzi SOAP per interagire con i servizi esportati.
Per ogni servizio esisterà quindi un componente software che da un lato si interfaccerà con l’utente attraverso il canale utilizzato, dall’altro invocherà via SOAP i servizi richiesti.

3.6 Componenti per la tracciabilità

Componenti per la tracciabilità
Il sistema di tracciabilità deve essere composto almeno dalle seguenti componenti:

- Log Server
- Sensori terminali locali
- Analizzatore di Log

Il **Log server** è il componente che implementa e gestisce la base di dati ove sono archiviati tutte le informazioni registrate per ogni transazione, operazione, ed accesso al sistema.
Tale server è tipizzato dal possedere meccanismi di ridondanza sui dati, atti a preservare possibili perdite di informazioni (tipicamente sistemi RAID); il server è inoltre dotato di meccanismi di backup periodico dei dati, sia su server di backup dedicati, che su supporti digitali (cdrom o DVD).

I **sensori terminali locali**, sono dei moduli software preposti a svolgere il compito di prelevare i dati relativi alla tracciabilità, nei punti del NAG in cui la transazione avviene. Tali dati saranno inviati al Log Server che provvederà ad archiviarli.
Come esempio esplicativo, può considerarsi la procedura di autenticazione; all’atto della presentazione delle credenziali utente, il sensore dovrà prendersi l’onere di contattare il Log server e di inviare i dati necessari prelevati durante la transazione.
I file di log locali relativi alla tracciabilità costituiscono essi stessi un riferimento valido al fine di gestire in modo ottimale il relativo servizio cui sono associati, e possono essere archiviati anche localmente se richiesto.
La comunicazione di dati tra i sensori terminali ed il server di monitoraggio deve avvenire su canale affidabile ed essere garantita.

L’ultimo elemento da considerare è una **stazione di analisi dei dati sui log** archiviati sul Log Server. I compiti svolti da questa stazione sono i seguenti:

- Generazione di report che espongano in modo leggibile risultati di analisi dei log, e che possono essere opportunamente modulati in funzioni delle informazioni che si vogliono estrarre dalla base di dati.
- Ricerca di informazioni.
- Console di amministrazione e gestione del Log Server.
- Stazione di registrazione su supporto ottico.

Per quanto riguarda la console di amministrazione, devono essere esplicitamente disponibili dei filtri per poter configurare dinamicamente le opzioni per il sistema e gli eventi da tracciare.
Tutti i dati devono essere interrogabili mediante un’interfaccia Web opportunamente realizzata.

3.6.1 I servizi da tracciare

I servizi erogati dal sistema sono caratterizzati da differenti livelli di criticità e responsabilità tra gli attori coinvolti nelle transazioni che risultano associate ad un servizio, siano essi utenti o enti. Si deve porre particolare attenzione alla tracciabilità e al monitoraggio di tutte le fasi di un ciclo di vita di un servizio:

- pubblicazione di un servizio,
- ricerca di un servizio,
- accesso ad un servizio.

L’esigenza di poter definire con precisione l’identità dei soggetti coinvolti, le responsabilità, oltre che la paternità delle azioni eseguite all’interno di una sessione di servizio, porta alla necessità di poter tracciare sia gli attori in gioco, sia la sequenza delle operazioni da questi svolte, durante la loro attività all’interno del sistema.
A valle di operazioni di autenticazione, il sistema deve memorizzare in opportuni archivi i tracciati di tutte le operazioni eseguite da un generico utente, sia esso:

- una persona fisica
- un sistema informatico (altro servizio)
- il gestore del servizi

Ad ogni operazione di accesso ad un servizio, devono obbligatoriamente essere associati i riferimenti a:

- Soggetto che la richiede
- Soggetto che la esegue
- Data esecuzione
- Esito della operazione
- Informazioni sullo stato del sistema

Ad ogni operazione relativa ad un servizio, devono obbligatoriamente essere associati i riferimenti a:

- dati relativi alla pubblicazione (inclusa l’accettazione dell’autorità di registrazione dei servizi),
- registro in cui è avvenuta la pubblicazione,
- Data esecuzione

- Esito della operazione
- Informazioni sullo stato del sistema.

3.7 Componenti per il monitoraggio

Per implementare un sistema di monitoraggio concertato nei termini esposti, i componenti richiesti sono i seguenti:

- Server di monitoraggio
- Sensori terminali locali
- Analizzatore di Log

Il **Server di monitoraggio** è il componente che implementa e gestisce la base di dati ove sono archiviate le informazioni raccolte da tutti i sensori di monitoraggio distribuiti tra le varie componenti del sistema. Tutti i dati registrati per ogni transazione, operazione, ed accesso al sistema.
Tale server è tipizzato dal possedere meccanismi di ridondanza sui dati, atti a preservare possibili perdite di informazioni (tipicamente sistemi RAID); il server è inoltre dotato di meccanismi di backup periodico dei dati, sia su server di backup dedicati, che su supporti digitali (cdrom o DVD) .

I **sensori terminali locali**, sono dei moduli software preposti a svolgere il compito di prelevare i dati relativi al monitoraggio, nei sistemi che effettuano monitoraggio, locale o cooperativo. Tali dati saranno inviati al Server di monitoraggio che provvederà ad archiviarli.
I sensori risiedono localmente ove il monitoraggio avviene (locale o cooperativo).

I dati devono essere archiviati localmente ed inviati periodicamente al Server di monitoraggio centralizzato.
Lo sforamento delle soglie imposte dagli SLA di riferimento, fa generare ai sensori terminali dei segnali di alert che vanno inviati al Server di monitoraggio, e nel caso di alert relativo al monitoraggio cooperativo anche al sistema monitorato che presenta una violazione critica degli SLA dichiarati.
La comunicazione di dati tra i sensori terminali ed il server di monitoraggio deve avvenire su canale affidabile ed essere garantita.
I file di log locali relativi al monitoraggio costituiscono essi stessi un riferimento valido al fine di gestire in modo ottimale il relativo servizio cui sono associati, e possono essere archiviati anche localmente se richiesto, oltre che obbligatoriamente essere spediti al Server di Monitoraggio centralizzato.

Come per la tracciabilità, l’ultimo elemento da considerare è una stazione di analisi dei dati archiviati sul Server di Monitoraggio. I compiti svolti da questa stazione sono i seguenti:

- Generazione di report che espongano in modo leggibile risultati di analisi dei dati, e che possono essere opportunamente modulati in funzioni delle informazioni che si vogliono estrarre dalla base di dati.
- Ricerca di informazioni.
- Console di amministrazione e gestione del Server di Monitoraggio
- Stazione di registrazione su supporto ottico
- Sistema di monitoraggio dei nodi attivi

Tutti i dati devono essere interrogabili mediante un’interfaccia Web opportunamente realizzata.

3.7.1 Componenti per il Monitoraggio operativo della qualità dei servizi

Il Sistema che consideriamo è un modello cooperativo e interoperabile, e conseguentemente può prevede l’interazione tra più domini, al fine di poter completare un servizio richiesto; in tale scenario i livelli caratterizzanti il servizio sono funzione dei singoli componenti che compongono la catena necessaria a completare una richiesta.
L’attività di monitoraggio è funzionale all’esigenza di caratterizzare con un elevato standard qualitativo i servizi erogati sia dal NAG che dagli NDOM.
La formalizzazione dei livelli di servizio attesi (Service Level Agreement) è definita nella Sezione 6, dove sono anche indicati, quali sono, nello specifico, i parametri qualitativi e quantitativi che devono essere soddisfatti dai servizi offerti dal NAG.

Per garantire che i sistemi rispettino gli SLA richiesti è necessario implementare un sistema di monitoraggio che garantisca un’attività continua di sorveglianza e mantenga traccia di quanto monitorato.
Il monitoraggio deve verificare che i sistemi tengano fede a quanto dichiarato in termini di SLA e che, in presenza di cambiamenti del sistema o aumento del carico, siano rilevati eventuali discostamenti dagli SLA richiesti.
Il monitoraggio è dunque finalizzato a mantenere alta la qualità del sistema e rilevare, ove si verificassero, decadimenti delle prestazioni o dell’affidabilità dei sistemi.

Il monitoraggio deve attuarsi sia a livello di NAG che di NDOM, a tal proposito occorre precisare che gli SLA definiti nel Capitolo 6 sono relativi ai servizi base e di aggregazione del NAG, oggetto della fornitura, mentre, per i servizi offerti dagli NDOM, il sistema di monitoraggio deve essere predisposto alla integrazione delle informazioni ottenute dai sistemi di monitoraggio locali, al fine di verificare se il livello di qualità raggiunto nell’erogazione del servizio, corrisponda a quello atteso, dichiarato dall’erogatore di servizio in fase di pubblicazione dello stesso.
Discorso analogo vale per i parametri che caratterizzano il sistema di comunicazione; anche in questo caso non è possibile monitorare direttamente i parametri della rete, in quanto dipendenti da numerosi fattori esterni al NAG, tuttavia, se il servizio viene erogato da un NDOM interconnesso alla rete mediante il Sistema Pubblico di Connettività che prevede delle attività di monitoraggio, deve essere possibile integrare i parametri sulla qualità del servizio del sistema di comunicazione, ottenuti da sistema di monitoraggio del Sistema Pubblico di Connettività (SPC), per consentire una valutazione più completa della qualità dei servizi aggregati in termini di tempo di risposta complessivo e tempo di risposta della rete di comunicazione.

Alla luce di quanto detto, deve essere possibile identificare e monitorare eventuali colli di bottiglia nel processo, che parte dal NAG ove tipicamente si accede, e procede fino all’ultimo stadio ove il servizio è poi realmente eseguito; inoltre è necessario avere a disposizione l’informazione relativa allo stato degli altri nodi NAG “attivi” nel sistema, disponibili a cooperare. Tale funzionalità deve poter essere attivata sempre dai gestori del sistema. Quanto detto, implica la necessità di operare il monitoraggio in due modalità distinte:

- Monitoraggio locale
- Monitoraggio cooperativo

Il **monitoraggio locale** è preposto a rilevare i dati concernenti i livelli di servizio richiesti al sistema stesso

Il **monitoraggio cooperativo** è invece rivolto a registrare i livelli di servizio attesi, dichiarati dai sistemi con cui si coopera.

Nel secondo caso, se ad esempio un determinato sistema fornitore dichiara una certa latenza del servizio, un sistema richiedente deve monitorare e registrare i tempi di latenza effettivi rispetto a quelli dichiarati dal sistema erogatore e dal sistema di rete.

Per l’attività di monitoraggio il sistema deve registrare in opportuni archivi i dati di tutte le operazioni eseguite dal sistema monitorato (sia locale che del sistema con cui si coopera) riportando le seguenti informazioni:

- Sistema che monitora
- Sistema monitorato
- SLA di riferimento
- Livelli di servizio rilevati
- Violazioni dei SLA
- Data rilevazione
- Esito sulla riuscita
- Informazioni sullo stato del sistema.

Le funzioni di monitoraggio devono poter essere richieste in modo interattivo dal gestore del sistema per verificare le prestazioni del sistema o condizioni di funzionamento anomalo.

3.8 Vincoli architetturali minimi

La piattaforma deve essere realizzata attraverso un’ architettura modulare, in modo da facilitare l’integrazione di nuove componenti tecnologiche, come ad esempio quelle necessarie per l’inserimento di nuove tipologie di terminali o di nuove componenti dello stack dei protocolli Web Services, in particolare, occorre:

- Consentire l’accesso ai servizi alle varie tipologie di terminali indipendentemente dalla loro natura, tenendo conto ovviamente delle limitazioni tecnologiche dei vari dispositivi.

- Garantire una qualità del servizio adeguata alle caratteristiche del terminale/client utilizzato per l’accesso al sistema e conforme al profilo dell’utente.

- Offrire funzionalità di accesso alle informazioni, tramite le quali l’utente possa avere la possibilità di scoprire dinamicamente i servizi offerti e tali da rendere il loro utilizzo una procedura quanto più possibile automatica.

- Fornire uno strato di sicurezza ed autenticazione degli utenti.

Data la complessa articolazione dei servizi previsti nel sistema, è richiesto che la Impresa fornitrice distribuisca, anche per ragioni di sicurezza, i vari servizi su macchine server diverse.

Tutti i server dovranno essere opportunamente dimensionati in numero, nella potenza elaborativa, nella memoria centrale, nella memoria di massa, nei dispositivi di I/O e nelle soluzioni architetturali per sostenere il carico dell’intero sistema garantendo livelli di servizio adeguati alle caratteristiche funzionali delle applicazioni in termini di tempi di risposta, quantità di dati gestita, affidabilità, scalabilità, continuità del servizio, sicurezza, etc. Il dimensionamento del sistema

deve essere fatto anche considerando i parametri di qualità del servizio descritti in un successivo capitolo.

3.8.1 Architettura fisica minimale

Data la complessa articolazione dei servizi previsti nel sistema, è richiesto che la Ditta aggiudicataria distribuisca, anche per ragioni di sicurezza, i vari servizi (accessibili anche singolarmente mediante l’uso di API) su diversi sistemi fisici. In particolare, si richiede che per implementare le componenti architetturali delle funzioni di base del NAG per lo sviluppo della cooperazione applicativa, descritte nel precedente paragrafo, vengano forniti almeno i seguenti sistemi fisici distinti descritti nei prossimi paragrafi; tali sistemi possono essere organizzati secondo modelli architetturali che prevedono l’integrazione di uno o più server per la realizzazione di ogni componente funzionale dell’architettura. Per le componenti descritte nei paragrafi precedenti, per le quali non è previsto uno specifico sistema, l’Impresa fornitrice si può riservare di proporre sia soluzioni basate sull’utilizzo di ulteriori sistemi, che di allocare opportunamente le componenti su uno dei sistemi previsti per altri componenti non pregiudicandone prestazioni e funzionalità.
Inoltre, le soluzioni che limitano lo spazio fisicamente occupato dai sistemi ad esempio con l’uso di armadi rack, saranno preferite.

Tutti i sistemi, limitatamente alla componete elaborativa, devono essere almeno composti da 2 nodi bi-processore al fine di garantire opportune caratteristiche prestazionali e di affidabilità grazie alla ridondanza dei componenti architetturali.
In alternativa, ogni nodo bi-processore può essere sostituito da un numero di unità di elaborazione montate in diverse configurazioni tali da garantire prestazioni ed affidabilità equivalenti. Tale specifica deve essere considerata per tutti i sistemi salvo che non sia diversamente specificato. In particolare sono richiesti almeno i seguenti sistemi, che saranno successivamente specificati nei loro sottosistemi componenti:

- sistema per l’integrazione e l’interoperabilità;
- sistema per la gestione della sicurezza;
- sistema per l’accesso multicanale;
- sistema per la tracciabilità;
- sistema per il monitoraggio operativo della qualità dei servizi;

Si fa presente, come emergerà dalla descrizione, che con il termine sistema si è considerata l’aggregazione di più sistemi fisici (sottosistemi). Il termine sistema è stato scelto per evidenziare il concetto che ci si riferisce a componenti integrate utilizzabili anche in modo autonomo.
Tutti i sistemi devono essere completi nelle loro componenti hardware e software; più sistemi ed i relativi sottosistemi possono essere allocati fisicamente nello stesso posto in armadi rack.
Altri sistemi, per l’applicazione CUP, saranno specificati in un successivo capitolo.

Si fa esplicitamente notare che nei paragrafi che seguono vengono riportati i vincoli architetturali minimi che devono essere soddisfatti per i vari sistemi individuati, mentre la valutazione della fornitura verrà fatta sulla base di tutte le componenti offerte e del modo in cui queste verranno integrate ed allocate per fornire tutte le funzionalità richieste, secondo quanto specificato nel Capitolato Speciale.

Prima di passare alla descrizione dei componenti fisici minimali, è importante tener presente che il NAG è composto da più componenti e, nel suo complesso, deve garantire elevati livelli di sicurezza perimetrale, integrando tutti i componenti e i meccanismi necessari alla realizzazione di un tale architettura. Allo scopo di garantire una ragionata ed efficace integrazione tra il sistema base e le componenti di sicurezza perimetrale, riportiamo nel paragrafo seguente sulla “Sicurezza perimetrale”, le componenti minime necessarie a garantire il raggiungimento di un efficace livello di sicurezza.

3.8.2 Sicurezza perimetrale

La sicurezza perimetrale è costituita da quell’insieme di meccanismi e componenti il cui scopo è quello di fornire all’*isola* dei componenti che costituiscono il sistema NAG, protezione contro minacce e violazione, sia esterne che interne. Tipicamente si parla di sistemi Firewall, IDS, Monitor di rete, Sistemi antivirus ed anti-spam.
Il dimensionamento del sistema di sicurezza perimetrale è imprescindibile dal sistema su cui deve operare, e per tal motivo non può essere definito una tantum, è necessario però definire direttive d’implementazione ed un set di controlli minimali che definiscono un modello di procedura da adottare nella realizzazione.
Tali specifiche non devono essere considerate vincolanti per tutti i domini del progetto, ma possono diventarlo in proporzione al livello di criticità assegnata agli asset individuati come risultato dei processi di Risk Assessment e Risk Management ed a quanto documentato nel documento sulle specifiche di sicurezza redatto in seguito a tali analisi, secondo quanto previsto in un successivo capitolo.
Per tale motivo le componenti architetturali preposte a svolgere mansioni pertinenti la sicurezza perimetrale devono essere tali da poter soddisfare nel loro insieme, e qualora un qualsiasi nodo del sistema lo richieda, ognuna delle seguenti direttive:

- deve supportare la comunicazione tramite i principali protocolli di sicurezza (SSL, TLS, HTTPS. IPSEC,…)
- deve poter comunicare tramite VPN con altri nodi.
- deve essere dotato di un firewall da interporre tre la rete interna ed il punto di accesso alla rete esterna.
- qualora siano presenti servizi pubblici erogati dal dominio, questi devono essere posti in zona Demilitarizzata. DMZ
- occorre diversificare rami della rete interna in funzione della tipologia dei sistemi presenti e dei livelli di criticità associati a tali sistemi, raggruppando i sistemi che presentano caratteristiche comuni, per dimensionare il tipo di protezione in funzione del tipo dei sistemi.
- occorre frammentare la rete in più tronconi separati tra loro da firewall per ridurre le probabilità di propagazione di un attacco, e proteggersi da eventuali attacchi interni.
- occorre proteggere con firewall dedicati, configurati opportunamente in modo mirato per zone del dominio che presentano degli asset da proteggere con caratteristiche diverse.
- occorre diversificare le tipologie di sistemi di sicurezza messi a guardia di un asset evitando ridondanze di sistemi simili.
- occorre l’adozione di sistemi di network ed host intrusion detection (IDS).
- i sensori IDS devono essere più di uno e vanno dislocati coerentemente alla topologia della rete; le posizioni critiche in cui posizionare tali sensori sono le seguenti:

  - Esternamente al border router
  - Tra il border router ed il firewall di primo livello
  - Dopo il firewall che protegge la DMZ
  - Dopo il firewall che protegge la intranet ed eventuali servizi di back end.
  - Sulla sottorete di monitoraggio ed amministrazione.
- occorre l’integrazione, su un unico canale comune, dei segnali di alert derivanti dai sistemi di monitoraggio e convogliarli verso un centro di monitoraggio.
- occorre prevedere una sottorete dedicata alle funzionalità di monitoraggio ed amministrazione.

3.8.3 Componenti fisici per l’integrazione e l’interoperabilità

In base a quanto visto nel paragrafo 3.3 sulle componenti dell’architettura, il sistema del NAG per lo sviluppo e la realizzazione di servizi per l’integrazione, deve includere almeno:

- Un sistema di Registry per la pubblicazione dei servizi e i componenti software che esportano le funzionalità del registro:
  - Un sistema di supporto alla realizzazione dei servizi aggregati,
  - Un sistema per la autorità per la registrazione dei servizi che offre le funzionalità definite precedentemente.
- Un sistema di supporto alla cooperazione dei servizi (sia EDA che SOA):
  - Un sistema per la gestione della busta di e-government;
- Un sistema per Web server operante in sicurezza;
- Un sistema per Web services operante in sicurezza,
- Un sistema per la gestione dei dati che include la archiviazione, sistemi di back-up e di mirroring.
- Un sistema per il file sharing (almeno 2 nodi sever bi-processore ed un array disk);
- Uno sistema di Proxy ed un sistema di Web caching (almeno 2 server bi-processore con un opportuno sistema di gestione dell’I/O);
- Un sistema per l’ambiate di sviluppo di nuove applicazione e per consentire i test (almeno 3 nodi bi-processore);
- Un sistema di DataBase Server con il software in grado di garantire la compatibilità con altri sistemi utilizzati in Regione (4 nodi con 8-processori ed un array disk);
- 10 Terminali client per l’accesso alla piattaforma dotati di dispositivi smartcard e lettori biometrici. Tali sistemi possono essere anche in configurazione con singolo nodo di elaborazione monoprocessore;
- Un sistema di stampa (almeno un server di stampa e 2 stampanti ad elevata risoluzione).

- Devono essere previsti apparati di rete (layer 2 e 3) che permettano la realizzazione di una infrastruttura di rete a larga banda per la interconnessione delle componenti del NAG e per l’integrazione con piena compatibilità della piattaforma nella intranet regionale:
  - Router
  - Switch
  - Access Point
  - Terminale di configurazione-controllo

- Armadi rack

- Gruppi di continuità

Tutti i sistemi devono essere completi nelle loro componenti hardware e software.

3.8.4 Componenti fisici per la gestione della sicurezza e del controllo degli accessi

I componenti fisici per la gestione della sicurezza, prevedono almeno i seguenti sistemi:

- Un sistema per una Infrastruttura a Chiave Pubblica:
  - Certification Authority ad uso interno per il rilascio ed il controllo di validità di certificati X.509 per gli utenti, i sistemi ed il software utilizzato;
  - Attribute Authority distribuite e ad uso interno per il rilascio ed il controllo di validità di certificati di attributo per utenti, i sistemi ed il software utilizzato;
- Un sistema per una Time Stamp Authority a validità interna, per il rilascio ed il controllo di validità di marche temporali e l’apposizione di timestamp per la certificazione delle richieste e dei documenti gestiti dal sistema
- Un sistema per la Gestione della sicurezza delle risorse che include almeno:
  - Un Application Server per ospitare i moduli software preposti al Controllo degli Accessi (Modulo autenticatore, Modulo Verifica Privilegi, Modulo Costruttore Profili, Modulo Controllore Policy);
  - Un Policy Manager;
  - Un sistema per il monitoraggio e gestione delle componenti costituenti l’infrastruttura di sicurezza che include: Log Server e strumenti di Log analysis, sistemi software per l’Auditing, Gateway dei segnali di alert provenienti dai sistemi di monitoraggio.
- Uno o più sistemi Proxy ed un sistema di Policy caching (almeno 2 server bi-processore);
- Un sistema LDAP.
- Un Firewall per ogni sottorete o dominio di rete che richieda differenti livelli di sicurezza.
- Sistema completo IDS compreso di sensori e terminali e stazione di monitoraggio.
- Dispositivi di archiviazione hardware dedicati per l’archiviazione delle chiavi private delle autorità di certificazione e di time stamping.
- 100 Dispositivi di sicurezza per i terminali client (Lettori e supporti smart-card)

- Devono essere opportunamente previsti apparati di rete (layer 2 e 3) che permettano la realizzazione di una infrastruttura di rete a larga banda per la interconnessione delle componenti di sicurezza e per l’integrazione con piena compatibilità della piattaforma nella intranet regionale:
  - Router
  - Switch
  - Access Point
  - Terminale di configurazione-controllo

- Armadi rack

- Gruppi di continuità

3.8.5 Componenti fisici per la gestione dell’accesso multicanale

I componenti fisici per la gestione dell’accesso multicanale prevede un **sistema di front-end** composto da:

- Componenti hardware e software per gestire i moduli per l’accesso multicanale.
- Componenti software per gestire i moduli di personalizzazione dell’accesso.

3.8.6 Componenti fisici per la gestione della tracciabilità

I componenti fisici per la gestione della Tracciabilità, prevedono le seguenti componenti:

- Un sistema per la Stazione centralizzata di gestione ed analisi dei Log che comprende:
  - Un sottosistema di Log Server,
  - Un sottosistema di Sensori terminali locali,
- Apparati di rete che permettano l’integrazione del sistema

3.8.7 Componenti fisici per la gestione del Monitoraggio qualitativo dei sistemi

I componenti fisici per la gestione del Monitoraggio qualitativo dei sistemi, prevedono le seguenti componenti:

- Un sistema per la Stazione centralizzata di gestione ed analisi dei Log che comprende:
  - Un sottosistema di Server di monitoraggio,
  - Un sottosistema di Sensori terminali locali,
- Apparati di rete che permettano l’integrazione del sistema

4 Caratterizzazione del Contesto e Scenari d’uso applicativi.

4.1 Premessa: il contesto operativo

Nei paragrafi precedenti sono state descritte le principali componenti del sistema per la realizzazione di una infrastruttura informatica per garantire la piena interoperabilità e cooperazione applicativa dei diversi sistemi delle strutture appartenenti al territorio regionale e/o operanti nella infrastruttura di rete regionale. Tale realtà risulta essere particolarmente complessa, sia in termini organizzativi che tecnologico-infrastrutturali.

La scelta di un modello di cooperazione esteso e generale, deve portare alla realizzazione di un'unica interfaccia che erogherà in modo omogeneo e trasparente, sia contenuti che servizi.

Lo scenario d’uso di una tale infrastruttura, vista l’articolata natura delle componenti in gioco e la molteplicità degli elementi impiegati, si svolge inevitabilmente su vari percorsi che vanno realizzati valutando opportunamente ad ogni livello, i parametri che intervengono nei processi interessati.
Di seguito verranno esposti fattori e variabili che caratterizzano il progetto, i requisiti e le specifiche sia tecnologiche che architetturali, che devono essere soddisfatte. A completamento

del quadro si elencano gli scenari d’uso del sistema per chiarire le differenti modalità operative che il sistema deve essere in grado di supportare.

4.2 Caratterizzazione del contesto

4.3 Scenari d’uso

In questo paragrafo si descrivono alcuni scenari d’utilizzo della piattaforma per meglio illustrare tutte le funzionalità in termini di integrazione, aggregazione e sicurezza. Gli scenari descrivono dei meccanismi di interazione che potranno essere ulteriormente definiti nel corso della realizzazione della piattaforma o nella successiva fase di sperimentazione, caratteristica di flessibilità che la piattaforma deve consentire di poter rendere agevolmente implementabile. L’analisi degli scenari fornisce un elemento concreto per determinare la complessità del sistema.

I casi d’uso che descriveremo sono tre:

CASO A: meccanismi di integrazione di un sito web esistente nella piattaforma;

CASO B: meccanismi di integrazione di un web server creato ad hoc per la piattaforma (cioè coerente con tutti i protocolli e standard definiti) e accessibili da Web, Web Services o da API;

CASO C: meccanismi di integrazione di un servizio legacy adattato con appositi adapter.

In realtà i servizi del caso C, una volta “wrappati” in un service provider sono trattati come nel caso B per cui non saranno discussi nel dettaglio ma era giusto inglobarli nella classificazione.

CASO A: meccanismi di integrazione di un sito web esistente nella piattaforma

Nel caso di integrazione di web server, la piattaforma deve essere in grado di integrare ogni servizio precedentemente realizzato garantendo al contempo gli stessi requisiti di sicurezza offerti dalla piattaforma, sia per quanto riguarda la personalizzazione del servizio in funzione della modalità d’accesso che per quanto riguarda la sicurezza dell’accesso. In tal caso sono necessari meccanismi che consentano l’accesso anche attraverso una rete sicura, realizzata mediante meccanismi di rete privata o mediante protocolli sicuri come l’SSL (Secure Socket Layer) e meccanismi per la personalizzazione basati su profili d’utente.

In questo caso è possibile individuare diverse modalità di integrazione in funzione del fatto che il sito web prevedeva o meno dei meccanismi di sicurezza.

Modello autonomo

Il Modello autonomo di autenticazione/autorizzazione è caratterizzato dal fatto che non esiste cooperazione tra i sistemi di autenticazione locale e centralizzato (leggi domini periferici e nodo aggregatore).
In altri termini quando l’utente accede ad un dominio è questi che si fa carico, se previsto, di richiedere e validare le credenziali dell’utente, in modo autonomo l’uno dall’altro.
Autenticazione ed autorizzazione sono entrambe gestite localmente, nel caso la transazione dovesse coinvolgere più domini, le credenziali possono essere richieste da ogni dominio.

Nel seguito vengono esposti gli scenari d’uso, relativi al Modello Autonomo.

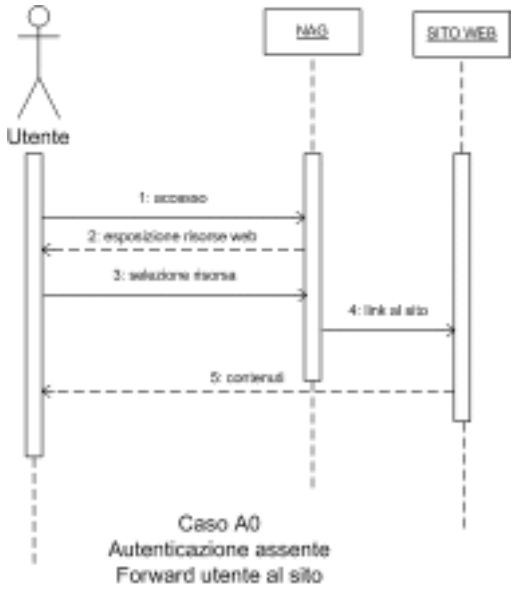
Nel caso in cui il sito in origine NON prevedeva un meccanismo di autenticazione, dopo la integrazione nella piattaforma di accesso, le possibilità sono due:

1. continua a non avere un meccanismo di controllo degli accessi -> AO
2. si affida al meccanismo di controllo degli accessi sul NAG -> A2

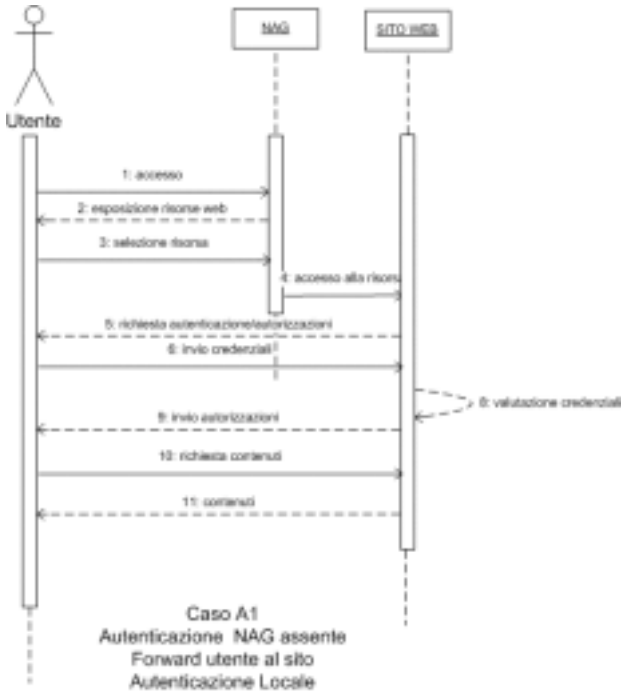
Nel caso in cui il sito in origine aveva dei meccanismi proprietari di autenticazione, la piattaforma può o meno implementarne altri di “più alto livello”, anche in questo caso le possibilità sono due:

1. Il controllo di accesso avviene unicamente sul sito locale -> A1
2. Il controllo di accesso avviene due volte, sia sul NAG che in locale -> A3

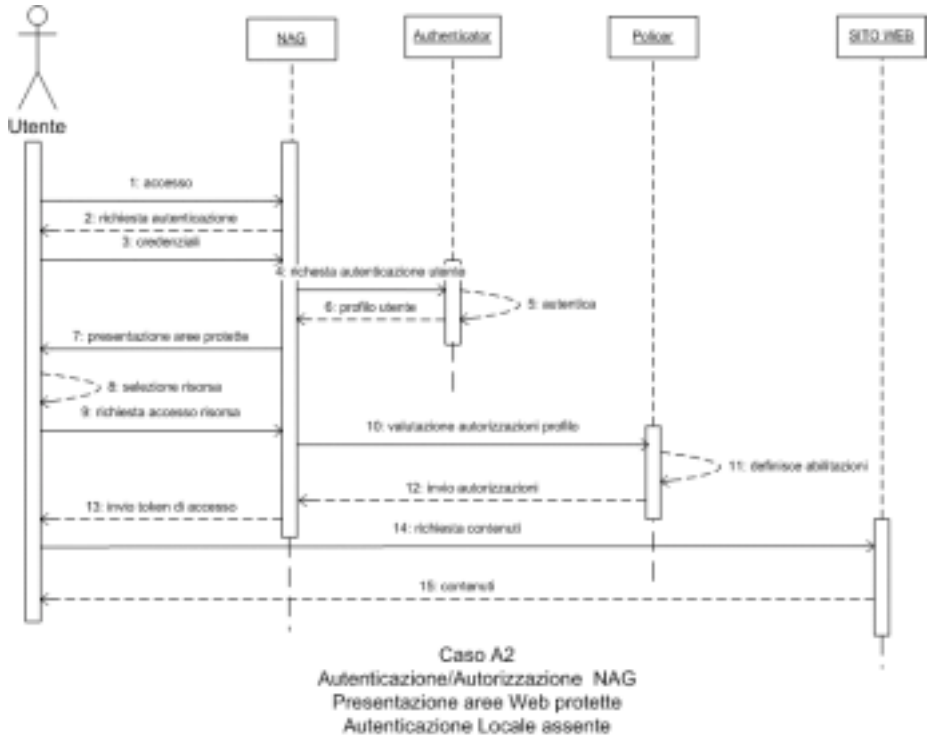
CASO A0 - il sito continua a non avere alcun meccanismo di sicurezza e la piattaforma si limita a forwardare la richiesta di accesso da parte di un utente direttamente alla risorsa;



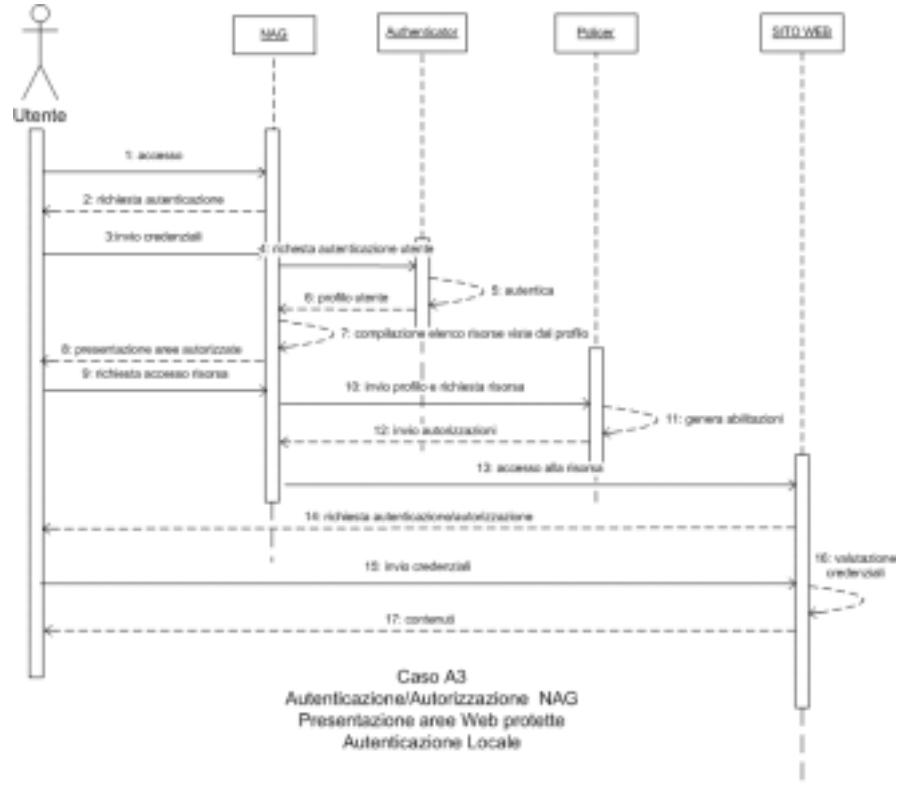
A1 -> la piattaforma forwarda la richiesta di accesso da parte di un utente direttamente alla risorsa che implementerà in maniera locale il suo meccanismo di sicurezza;



A2 -> la piattaforma d’accesso implementerà dei meccanismi di sicurezza prima di forwardare la richiesta alla risorsa (figura seqA2);

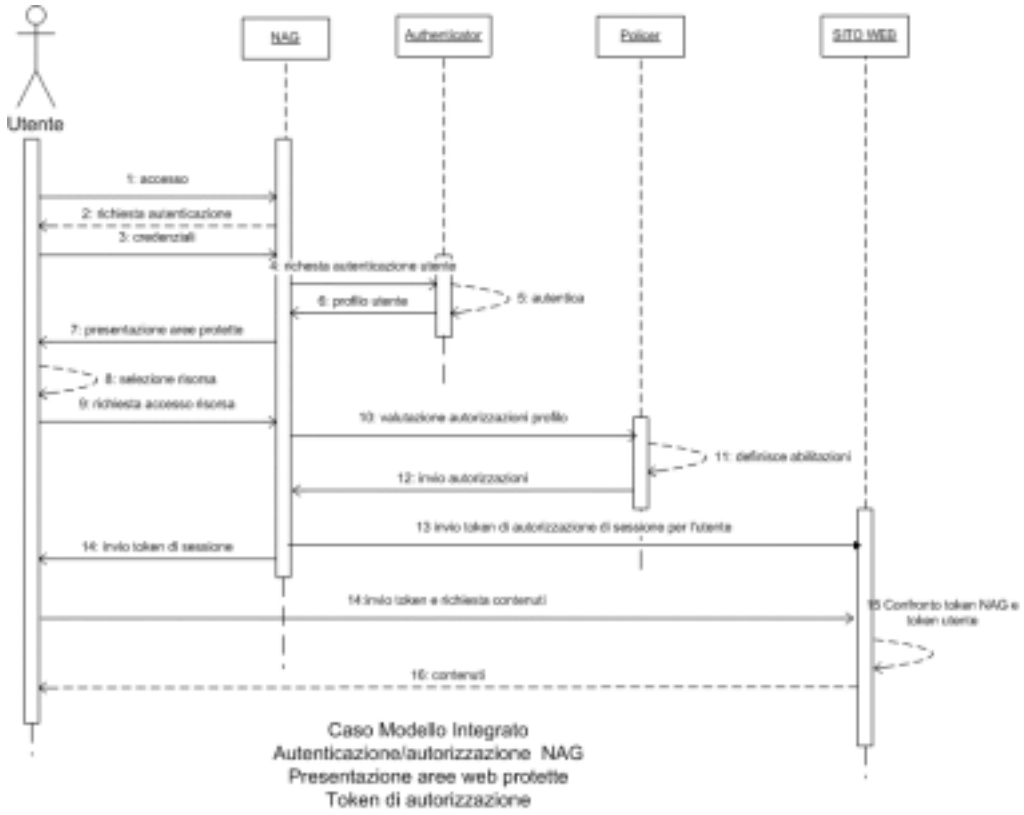


A3 -> la piattaforma d’accesso implementerà dei meccanismi di sicurezza prima di forwardare la richiesta alla risorsa che implementerà in maniera locale il suo meccanismo di sicurezza (figura seqA3);



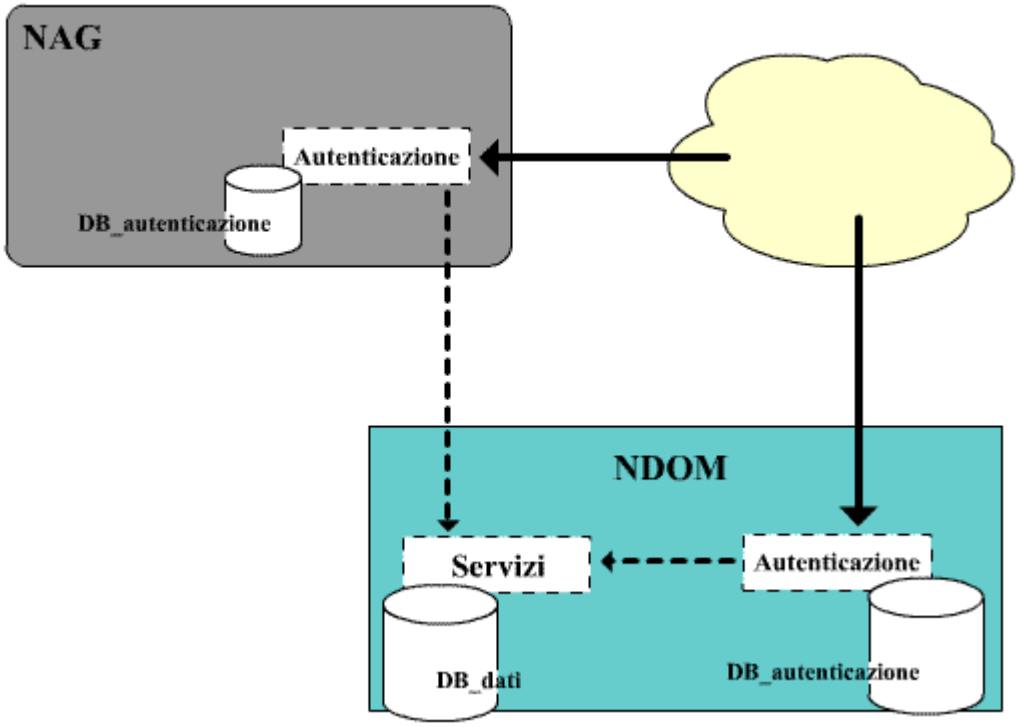
Modello integrato:

L’utente viene autenticato ed autorizzato sul NAG; come risultato positivo della autenticazione, all’utente viene fornito un token di sessione da utilizzare per accedere alla risorsa web richiesta. Il NAG invia anche alla risorsa un token associato all’utente che farà richiesta di accesso. Quando l’utente accederà alla risorsa, dovrà fornire il token personale che verrà confrontato con quello inviatogli dal NAG ed in caso di verifica positiva il servizio permetterà l’accesso all’utente.



CASO B e C: meccanismi di integrazione di un web server nella piattaforma

Nel caso di integrazione di web services, la piattaforma deve essere in grado di offrire entrambi i meccanismi di controllo degli accessi così come descritto nel modello di SPICCA e sinteticamente riportato in figura:



Descrizione logica del Sistema di autenticazione

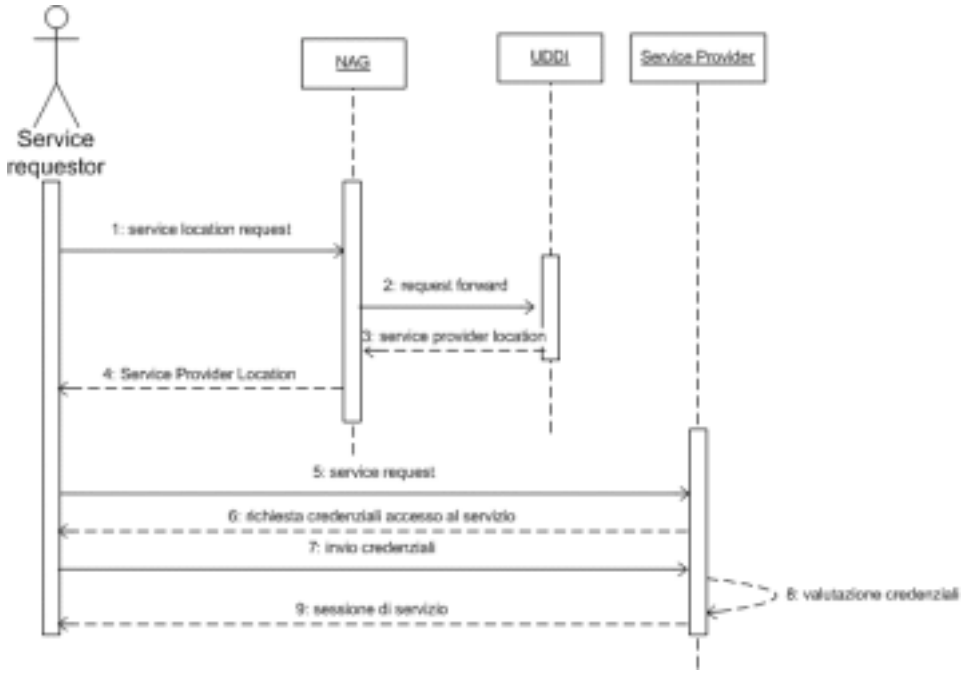
Nel primo caso, il policy manager agisce sul nodo erogatore; un tipico scenario operativo vede nella home page del nodo aggregatore i links verso i servizi e, solo all’atto dell’accesso ad uno di essi, potrà essere effettuata l’autenticazione dell’operatore in base alla registrazione dell’account dell’operatore nel database di autenticazione ed in base alle policy di autorizzazione del nodo erogatore.

Nel secondo caso il policy manager agisce sul nodo aggregatore ed il processo di autenticazione risulta essere centralizzato, quindi la gestione delle liste degli account e delle policy sarà implementata sulla conoscenza del nodo centrale, e solo dopo essere stato effettuato il riconoscimento dell’operatore, sarà possibile accedere ai nodi erogatori con la possibilità di fruire dei rispettivi servizi.

In definitiva è possibile individuare diverse modalità di integrazione in funzione del fatto che il sito web prevedeva o meno dei meccanismi di sicurezza:

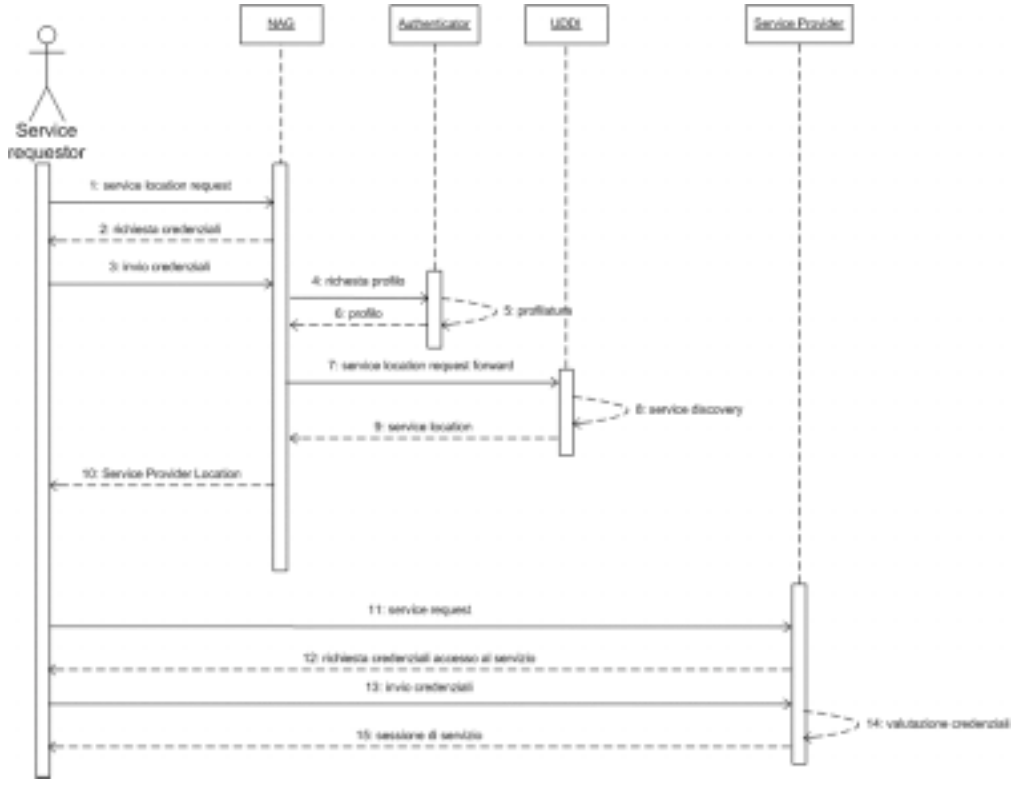
Modello autonomo

B0 -> la piattaforma forwarda la richiesta di accesso da parte di un service requestor al registro dei servizi (UDDI), una volta ottenuto l’URL del service provider vi accede direttamente e sarà soggetto ai meccanismi di autenticazione ed autorizzazione che il service provider implementa localmente.



B0

B1 -> la piattaforma autentica il service requestor (autenticazione sul NAG) poi forwarda la richiesta di accesso al registro dei servizi (UDDI), la lista dei servizi disponibili viene filtrata dalla piattaforma in base alle credenziali del service requestor (autorizzazione sul NAG), a questo punto la richiesta “autorizzata” viene inoltrata al service provider che può o meno attivare un secondo processo di autorizzazione locale.



B1

5 La realizzazione delle funzioni di aggregazione per il CUP sanitario della Regione Campania

5.1 Premessa

In aggiunta alla realizzazione delle funzioni di base per la cooperazione applicativa, la fornitura deve prevedere la realizzazione delle funzioni specifiche (livello applicativo) del nodo aggregatore (NAG) relative al Centro di Prenotazione Unico (CUP) sanitario della Regione Campania. Il nodo, ottenuto integrando i servizi di prenotazione disponibili presso le AASSLL e le aziende ospedaliere (AAOO), deve fornire un servizio di prenotazione integrato su tutte le disponibilità presenti in Campania. Tale attività è una concreta sperimentazione delle funzionalità del NAG per uno specifico servizio e si avvarrà dei risultati del progetto di adeguamento dei CUP degli Enti sanitari finanziato dalla Regione Campania, che ha consentito alle AASSLL e alle AAOO di omogeneizzare i propri sistemi di prenotazione. Gli Enti coinvolti sono circa 30.

Le funzioni base del Nodo Aggregatore e le funzioni specifiche relative al sistema CUP devono essere realizzate in due architetture fisicamente distinte che possano essere allocate in due diversi punti di accesso della rete della Regione Campania.

La sperimentazione consiste nel realizzare un nodo aggregatore che integri i servizi attualmente offerti dal CUP rendendoli visibili sia ad utenti esterni (presentandoli in maniera opportuna ai diversi tipi di utenti e terminali che richiedono i servizi del CUP) che ad altri Enti che richiedono i servizi del CUP.
I servizi da integrare saranno resi disponibili per ogni Ente coinvolto in due diverse modalità tramite: pagine web e accesso basato su tecnologie di tipo “web services”; per entrambe le modalità deve essere prevista l’integrazione nel NAG.

Si fa presente che gli Enti coinvolti nel CUP devono poter continuare ad offrire i propri servizi in autonomia indipendentemente dalle funzionalità previste per il nodo aggregatore.

Lo scenario che di seguito verrà illustrato mira a fornire la descrizione delle funzionalità, del formato dei dati e dell’architettura di riferimento dei sistemi CUP operanti presso le AASSLL e AAOO. Il nodo aggregatore deve offrire le stesse funzionalità previste da una singolo Ente (Consultazione Anagrafica Assisti,Consultazione Anagrafica Medici di Base, Prenotazione Prestazione, Cancellazione Prestazione e Visualizzazione Prestazione), consentendo come valore aggiunto di offrire in modo integrato l’accesso alle risorse sanitarie dell’intera Regione.

In aggiunta alle funzionalità base del CUP dovrà essere realizzata una funzione specifica per la ricerca multicriterio per individuare, in relazione alla richiesta dell’utenza, una o più offerte di servizi sanitari.
Il nodo aggregatore del CUP deve offrire due tipologie di servizi:

1. può comportarsi come semplice “Web Content Manager” il cui compito principale è quello di integrare pagine web esistenti realizzate dalle ASL e dagli Ospedali,
2. può offrire come servizio aggregato la possibilità di elaborare un algoritmo che implementa un predefinito criterio di ricerca per ottimizzare il risultato di una ricerca in funzione di un criterio stabilito quale può essere il tempo di attesa per una prestazione o la distanza della struttura dal richiedente.

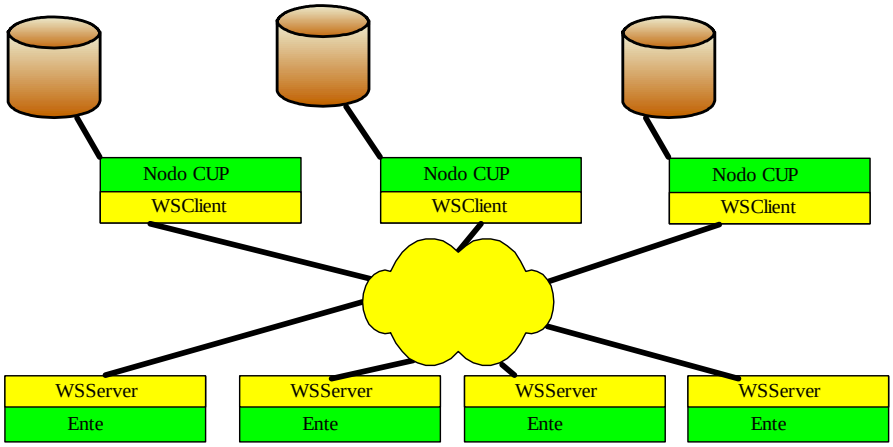
Le funzionalità previste, i protocolli e il formato dei dati potranno essere modificati nel corso della realizzazione o dell’esercizio, esse tuttavia devono sempre rispettare i livelli di servizio attesi così come esplicitamente definiti e richiesti nel Capitolo 6.

In definitiva, sono previste due diverse modalità di integrazione operanti sempre con i dovuti livelli di sicurezza:

- una prima che prevede la realizzazione di un sistema Web il quale, senza specifiche funzioni di integrazione delle risorse, sia solo un punto di accesso ai sistemi di prenotazione delle diverse aziende e di consultazione delle anagrafi. In pratica si avrebbe un punto unico per poter scegliere i servizi di un ASL e, con un’interfaccia omogenea, effettuare le prenotazioni. In questo caso è comunque richiesta un’autenticazione del sistema utilizzando anche i servizi base del NAG;
- una seconda che prevede la realizzazione di un portale che integri realmente le diverse risorse territoriali e permetta prenotazioni ad un sistema integrato rendendo trasparente l’interazione con i CUP dei singoli enti. In pratica in questo caso la richiesta parte dalle esigenze dell’utente e a fronte di queste verrebbero individuate le possibili offerte e successivamente effettuate le prenotazioni. Il sistema deve guidare la scelta con criteri di selezione (vicinanza, fascia oraria, etc.) ottenendo un portale di servizi strettamente integrati.

L’erogazione di tali servizi presuppone:

A. la presenza di una base di dati locale al nodo che si interfaccia con gli utenti e che in parte sia replicata sui nodi degli enti;
B. l’espletamento di tali attività presso gli enti che erogano effettivamente la prestazione all’assistito:



5.2 Funzionalità del CUP

Nell’ambito del progetto CUP, è stato definito in maniera congiunta da parte di tutte le AASSLL e le AAOO:

- l’insieme dei servizi/funzionalità di base che si intende implementare,
- le procedure applicative dei singoli servizi evidenziati,
- la struttura dei dati scambiati
- un layout comune delle interfacce.

I servizi/funzionalità che il CUP deve garantire, sono:

- Consultazione Anagrafica Assisti,
- Consultazione Anagrafica Medici di Base,
- Prenotazione Prestazione,
- Cancellazione Prestazione,
- Visualizzazione Prestazione.

Allo scopo di dare la possibilità di valutare la complessità del sistema, verranno di seguito descritti, in maniera esemplificativa, i servizi/funzionalità di “Consultazione Anagrafe Assistiti” e “Prenotazione Prestazione”. Per ognuna di esse, verranno date una descrizione informale del servizio, la sequenza dei passi relativi alla procedura che implementerà il servizio/funzionalità, una descrizione della struttura dei dati scambiati per il completamento della procedura e un’ipotesi di interfaccia comune orientata al Web; tutti i dettagli relativi alle specifiche funzionalità, verranno forniti successivamente.

In relazione alla strutture dati scambiati per il completamento delle procedure individuate, è stato definito l’insieme dei campi che costituiscono lo scambio informativo. Per ogni campo, è stato individuato l’obbligatorietà o meno dello stesso, il tipo e la dimensione del campo specifico. Inoltre, per conformarsi agli attuali standard in uso, si è provveduto ha verificare la corrispondenza con i campi del protocollo HL7, il quale rappresenta lo standard de facto per quanto concerne i sistemi informatici all’interno del mondo sanità a livello mondiale.

La progettazione e il disegno delle interfacce sono state svolte nell’intento di incrementare:

- il livello di usabilità
- la semplicità di utilizzo
- minimizzazione il grado di disorientamento delle utenze

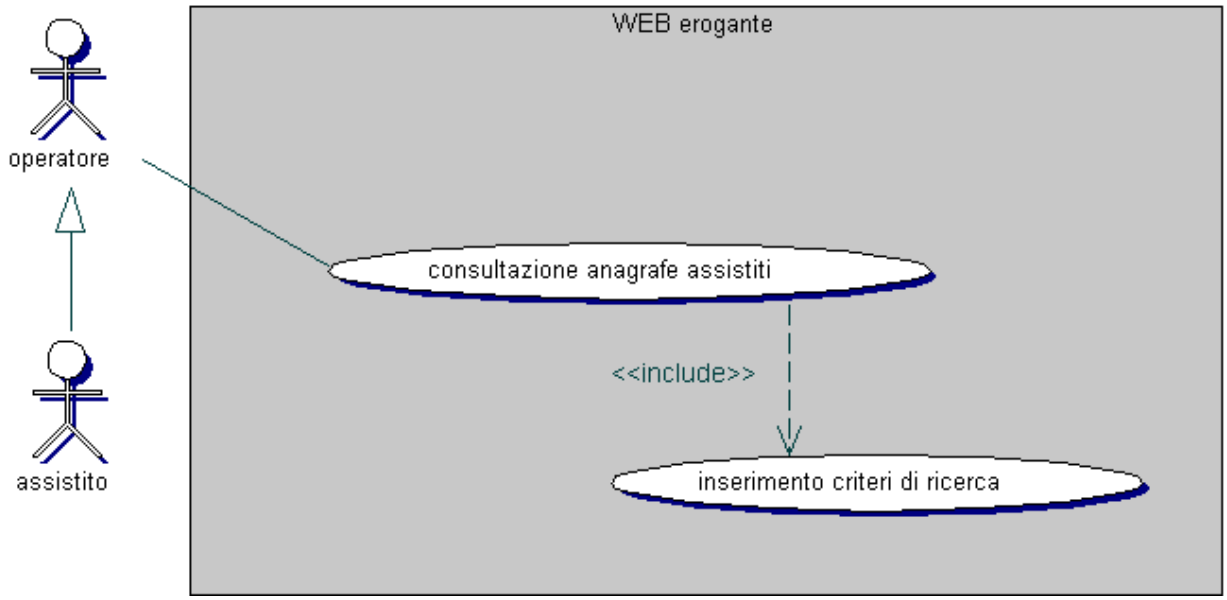
Consultazione Anagrafe Assistiti

Descrizione informale:
Tale procedura consente la consultazione delle anagrafiche degli assistiti. Tale funzione risulta particolarmente utile per una verifica incrociata dei dati e dei diritti degli assistiti.

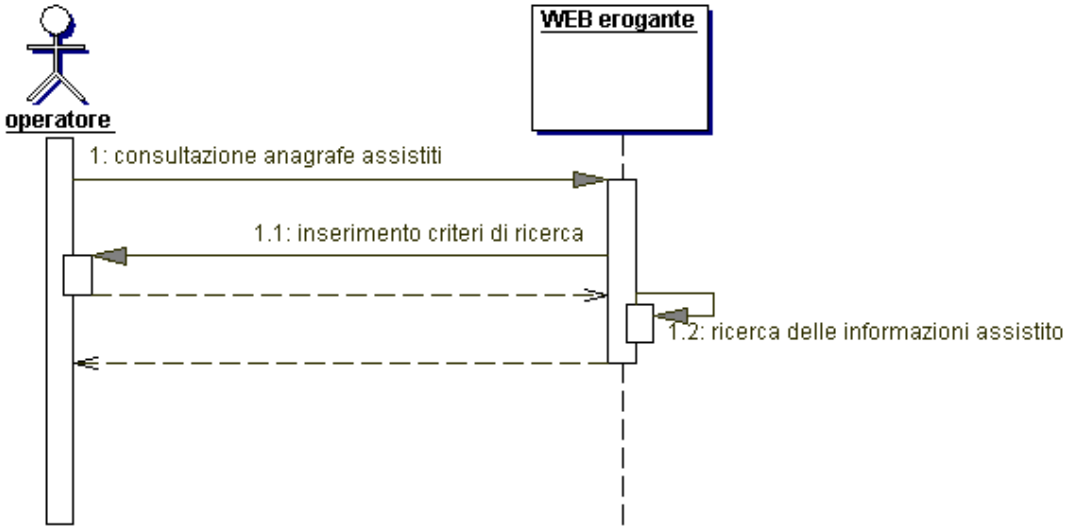
Passi della procedura:

1. Collegamento al sito dell’ente a cui si vogliono chiedere informazioni su un assistito
2. Inserimento delle informazioni dell’assistito
3. Consultazioni dell’anagrafica dell’ente consultato
4. Visualizzazione delle informazioni estratte dagli archivi

Use Case Diagram:



Sequence Diagram:



Situazioni di guasto /caduta:
Nessuna situazione è critica in quanto la procedura non comporta una modifica dello stato del sistema, ma solo una consultazione dei dati.

Tracciato dei Record informativi:

Richiesta informazioni assistito:

- **DTD**

```
<?XML VERSION="1.0" ENCODING="UTF-8"?>
<!ELEMENT RICHIESTA_INFORMAZIONI_ASSISTITO (ASSISTITO)>
<!ATTLIST RICHIESTA_INFORMAZIONI_ASISTITO
   IDCUP ID #REQUIRED
   IDOPERATORE ID #REQUIRED
```

```
   DATAORA CDATA #REQUIRED
>

<!ELEMENT ASSISITO (CODFISCALE, CODSANITARIO?, NOME?, COGNOME?, SESSO?, DATANASCITA?,
INDIRIZZO?, CITTA?, PROVINCIA?, CODPOSTALE?, STATO?, TELEFONO?, E-MAIL?)>
<!ELEMENT CODFISCALE (#PCDATA)>
<!ELEMENT CODSANITARIO (#PCDATA)>
<!ELEMENT NOME (#PCDATA)>
<!ELEMENT COGNOME (#PCDATA)>
<!ELEMENT SESSO (#PCDATA)>
<!ELEMENT DATANASCITA (#PCDATA)>
<!ELEMENT INDIRIZZO (#PCDATA)>
<!ELEMENT CITTA (#PCDATA)>
<!ELEMENT PROVINCIA (#PCDATA)>
<!ELEMENT CODPOSTALE (#PCDATA)>
<!ELEMENT STATO (#PCDATA)>
<!ELEMENT TELEFONO (#PCDATA)>
<!ELEMENT E-MAIL (#PCDATA)>
```

- **Descrizione dei campi**

Obb.	Nome	Tipo	Lung.	Descrizione	Valore	HL7 2.3.1 compliance
SI	idCup	N	9	Identificativo del sistema che effettua la richiesta		MSH.3
SI	idOperatore	AN	20	Identificativo dell’operatore che effettua la richiesta		MSH.4
SI	DataOra	N	12	La data e l’ora della richiesta	Formato: AAAAMMGGHHMI	MSH.7
NO	CodSanitario	AN	16	Codice Sanitario dell’assistito		PID.2
SI	CodFiscale	AN	16	Codice Fiscale dell’assistito		PID.4
NO	Nome	AN	48	Nome dell’assistito		PID.5.XPN.1
NO	Cognome	AN	48	Cognome dell’assistito		PID.5.XPN.2
NO	Sesso	AN	1	Identifica il sesso dell’assistito	Maschio = “M” Femmina = “F”	PID.8
NO	DataNascita	N	8	Data di nascita dell’assistito	Formato: AAAAMMGG	PID.7
NO	Indirizzo	AN	50	Indirizzo dell’assistito		PID.11.XAD.1
NO	Citta	AN	50	Citta dell’assistito		PID.11.XAD.3
NO	Provincia	AN	50	Provincia dell’assistito		PID.11.XAD.4
NO	CodPostale	AN	15	Codice postale o ZIP dell’assistito		PID.11.XAD.5
NO	Stato	N	10	Codice dello stato di appartenenza		PID.11.XAD.6
NO	Telefono	AN	25	Recapito telefonico per contattare l’assistito		PID.13.XTN.7
NO	E-mail	AN	30	E-mail dell’assistito		PID13.XTN.4

Risposta informazioni assistito:

- **DTD**

```
<?XML VERSION="1.0" ENCODING="UTF-8"?>
<!ELEMENT RISPOSTA_INFORMAZIONI_ASSISTITO (ASSISTITO*)>
<!ATTLIST RISPOSTA_INFORMAZIONI_ASISTITO
   IDCUP ID #REQUIRED
   DATAORA CDATA #REQUIRED
>

<!ELEMENT ASSISITO (CODFISCALE?, CODSANITARIO?, NOME, COGNOME, SESSO, DATANASCITA,
TIPOESENZIONE, INDIRIZZO?, CITTA?, PROVINCIA?, CODPOSTALE?, STATO?, TELEFONO?, E-MAIL?)>

<!ELEMENT CODFISCALE (#PCDATA)>
<!ELEMENT CODSANITARIO (#PCDATA)>
<!ELEMENT NOME (#PCDATA)>
<!ELEMENT COGNOME (#PCDATA)>
```

```
<!ELEMENT SESSO (#PCDATA)>
<!ELEMENT DATANASCITA (#PCDATA)>
<!ELEMENT TIPOESENZIONE (#PCDATA)>
<!ELEMENT INDIRIZZO (#PCDATA)>
<!ELEMENT CITTA (#PCDATA)>
<!ELEMENT PROVINCIA (#PCDATA)>
<!ELEMENT CODPOSTALE (#PCDATA)>
<!ELEMENT STATO (#PCDATA)>
<!ELEMENT TELEFONO (#PCDATA)>
<!ELEMENT E-MAIL (#PCDATA)>
```

– **Descrizione dei campi**

Obb.	Nome	Tipo	Lung.	Descrizione	Valore	HL7 2.3.1 compliance
SI	IdCup	N	9	Identificativo del sistema che genera la risposta		MSH.3
SI	DataOra	N	12	La data e l’ora della richiesta	Formato: AAAAMMGGHHMI	MSH.7
NO	CodSanitario	AN	16	Codice Sanitario dell’assistito		PID.2
SI	CodFiscale	AN	16	Codice Fiscale dell’assistito		PID.4
SI	Nome	AN	48	Nome dell’assistito		PID.5.XPN.1
SI	Cognome	AN	48	Cognome dell’assistito		PID.5.XPN.2
SI	Sesso	AN	1	Identifica il sesso dell’assistito	Maschio = “M” Femmina = “F”	PID.8
SI	DataNascita (Eta)	N	8	Data di nascita dell’assistito	Formato: AAAAMMGG	PID.7
SI	tipoEsenzione	AN	1	Identificativo dell’esenzione dell’assistito (significativo nel SSN)	Totale = “T” Parziale = “P” Nessuna = “N”	PV1.2
NO	Indirizzo	AN	50	Indirizzo dell’assistito		PID.11.XAD.1
NO	Citta	AN	50	Citta dell’assistito		PID.11.XAD.3
NO	Provincia	AN	50	Provincia dell’assistito		PID.11.XAD.4
NO	CodPostale	AN	15	Codice postale o ZIP dell’assistito		PID.11.XAD.5
NO	Stato	N	10	Codice dello stato di appartenenza		PID.11.XAD.6
NO	Telefono	AN	25	Recapito telefonico per contattare l’assistito		PID.13.XTN.7
NO	E-mail	AN	30	E-mail dell’assistito		PID13.XTN.4

Un’ipotesi si interfaccia WEB per la procedura che implementare il servizio/funzionalità “Consultazione Anagrafe Assistiti” è riportata nelle seguenti figure.

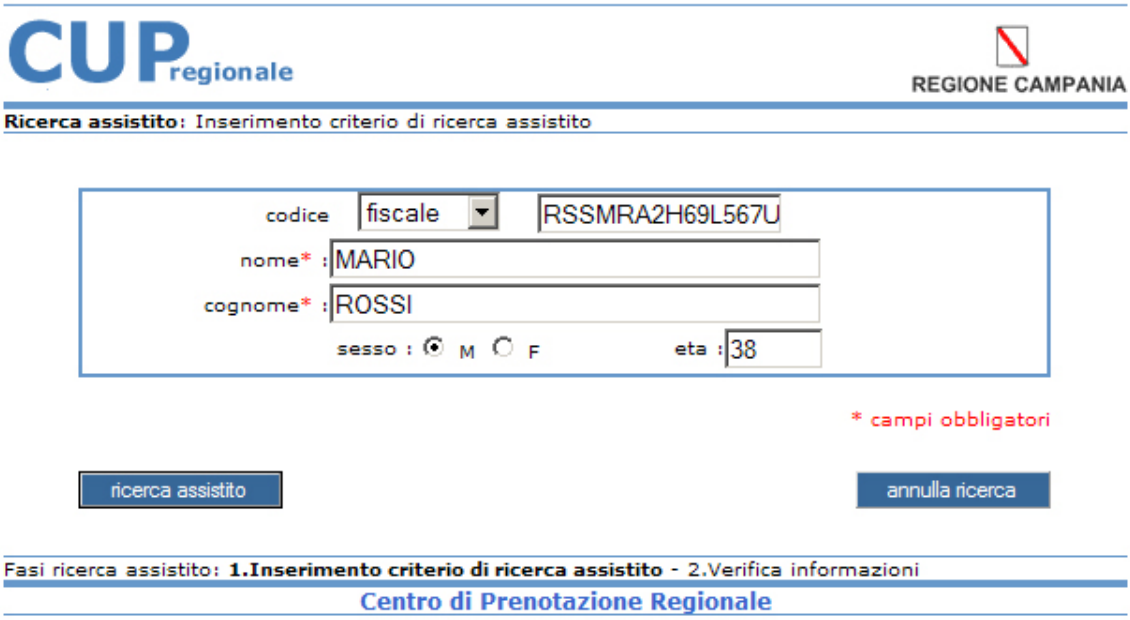


Figura 1 -inserimento criteri di ricerca

La prima interfaccia WEB immaginata è relativa all’inserimento dei criteri di ricerca per l’individuazione dell’assistito di interesse. In essa individuiamo tre aree fondamentali:

- Una posizionata in alto, in cui viene riportato un riferimento al passo della procedure attualmente in atto
- Una centrale, in cui sono riportati i form per l’immissione di criteri di ricerca
- Una in basso, in cui viene indicata la procedura in atto e i passi che la compongono

La suddivisione in tre aree sarà ripresa in tutte le interfacce, in cui l’area centrale potrà differenziarsi, in base alle necessità, come area in cui inserire o leggere le informazioni relative alla procedura di atto.

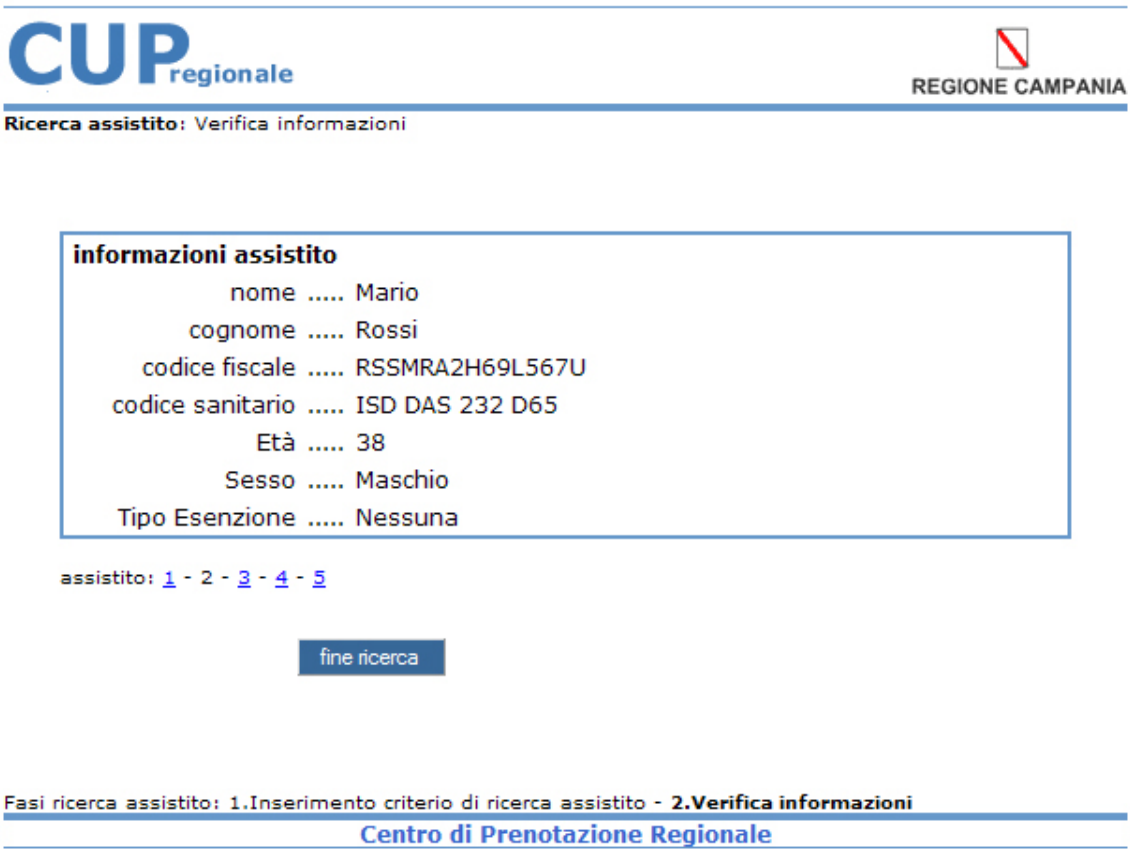


Figura 2 - visualizzazione delle informazioni

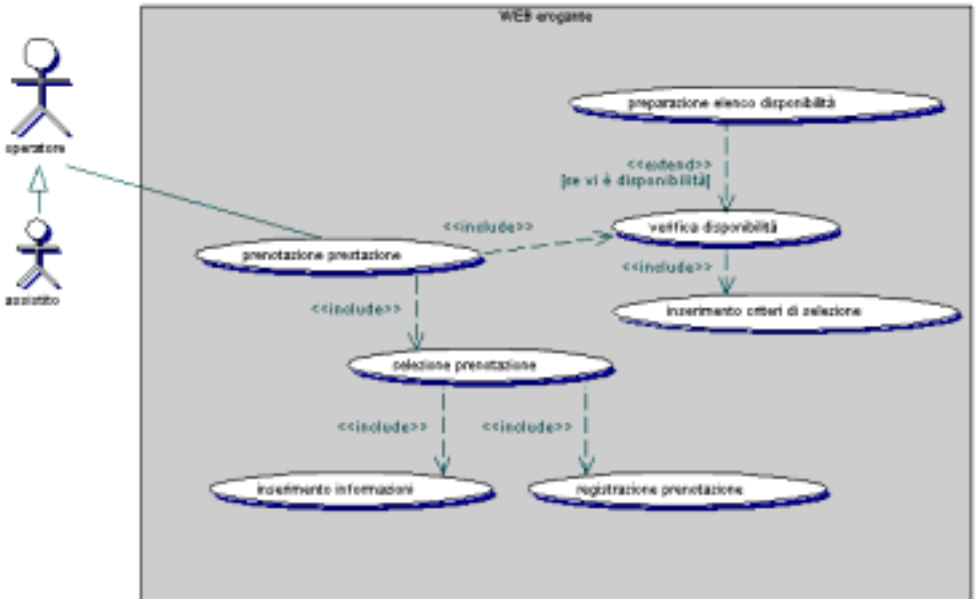
Prenotazione Prestazione

Descrizione informale:
Tale procedura consentirà, ad un operatore remoto, precedentemente autenticato, di effettuare una prenotazione in uno specifico ente di un suo assistito. Di seguito indicheremo con nodo R, il nodo del richiedente, e con nodo E il nodo erogante la prestazione.

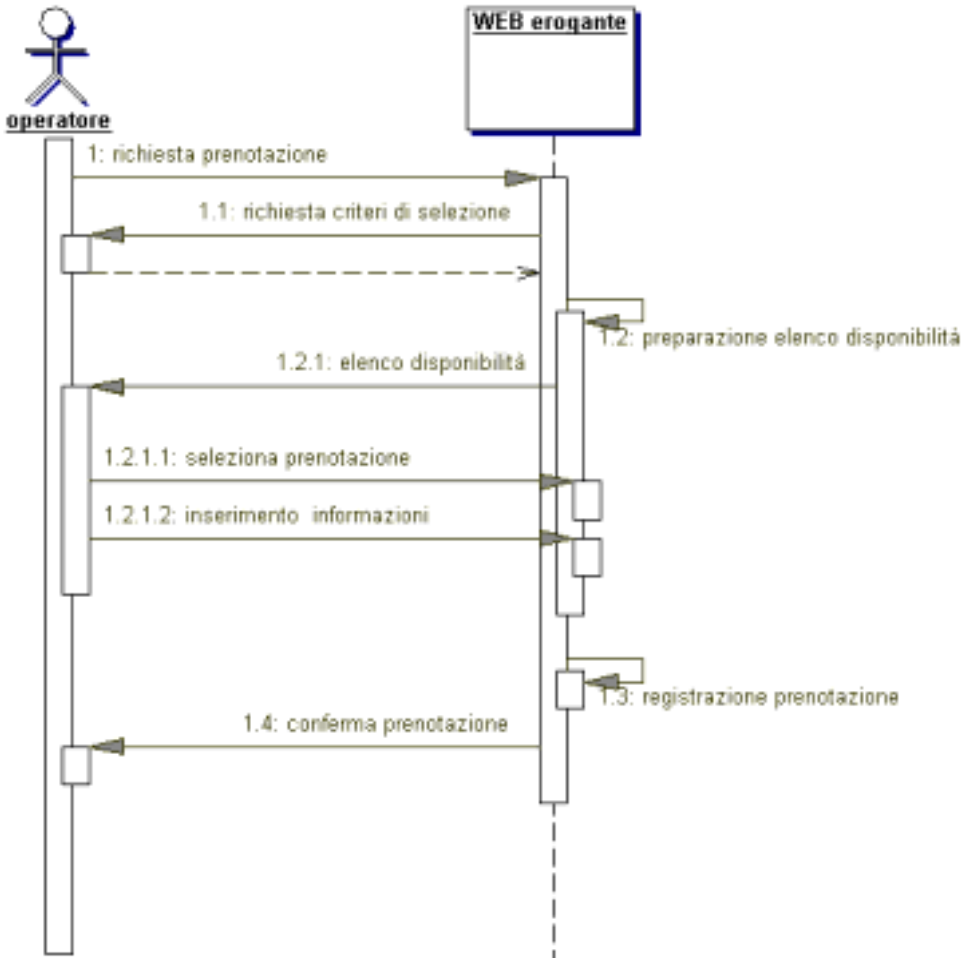
Passi della procedura:

- Collegamento al sito dell’ente a cui si vuole chiedere una prenotazione
- Verifica della disponibilità ad effettuare in base ai criteri di ricerca legati all’ASSISTITO, alla PRESTAZIONE e alle PREFERENZE dell’assistito
- Consultazione dell’elenco delle possibilità offerte dall’ente erogante
- Scelta dell’offerta di interesse e relativa richiesta di prenotazione
- Inserimento informazioni anagrafiche del proprio assistito e della prescrizione/impegnativa
- Visualizzazione della conferma di avvenuta prenotazione
- Stampa della scheda riassuntiva dell’appuntamento

Use Case Diagram:



Sequence Diagram:



Situazioni di guasto /caduta:

- Caduta del nodo R
    - Se avviene prima di effettuare la richiesta di prenotazione, non vi è criticità
    - Se avviene dopo aver effettuato la richiesta di prenotazione, ma prima di aver ricevuto la conferma, allora al riavvio del nodo sarà necessario consultare il sito del nodo E per verificare se la prenotazione è stata registrata o meno.
- Caduta del nodo E
    - Se avviene prima che il nodo R effettui la richiesta di prenotazione, non vi è criticità, poiché il nodo R prenderà atto della non disponibilità ed eventualmente attiverà una procedura di prenotazione verso un nodo differente da E.
    - Se avviene dopo che il nodo R ha effettuato la richiesta di prenotazione, ma prima che R riceva conferma, allora il nodo R dovrà attivarsi per:
        - Se potrà visionare le prenotazioni del sito del nodo E, controllerà l’effettuata prenotazione e operare di conseguenza.
        - Se non potrà visionare le prenotazioni del sito del nodo E, assumerà che la prenotazione non sia avvenuta e attiverà, per la coerenza del sistema, una procedura per la cancellazione della stessa ed eventualmente attiverà una procedura di prenotazione verso un nodo differente da E.

N.B.: per garantire la coerenza dell’informazione, si potrebbe anche ipotizzare di demandare ad un nodo di coordinamento (ad esempio il nodo Regionale) compiti di sincronizzazione delle informazioni; in tal caso le informazioni di prenotazione e cancellazione effettuate dai diversi nodi, saranno registrate anche nel nodo di coordinamento sfruttate da i singoli nodi per verificare l’allineamento delle proprie informazioni.

Tracciato dei Record informativi:

Richiesta disponibilità:

– **DTD**

```
<?xml version="1.0" encoding="UTF-9"?>
<!ELEMENT RICHIESTA_DISPONIBILITA (ASSISTITO?, PRESTAZIONE, PREFERENZE?,
MaxRisposte?)>
<!ATTLIST RICHIESTA_DISPONIBILITA
    idCUP ID #REQUIRED
    idOperatore ID #REQUIRED
    DataOra CDATA #REQUIRED
>

<!ELEMENT ASSISTITO (tipoEsenzione?, Sesso?, DataNascita?, Urgenza?)>
<!ELEMENT tipoEsenzione (#PCDATA)>
<!ELEMENT Sesso (#PCDATA)>
<!ELEMENT DataNascita (#PCDATA)>
<!ELEMENT Urgenza (#PCDATA)>

<!ELEMENT PRESTAZIONE (idPrestazione)>
<!ELEMENT idPrestazione (#PCDATA)>

<!ELEMENT PREFERENZE (idStruttura?, idUnitaErogante?, daGiorno?, aGiorno?, Orario?)>
<!ELEMENT idStruttura (#PCDATA)>
<!ELEMENT idUniàErogante (#PCDATA)>
<!ELEMENT daGiorno (#PCDATA)>
<!ELEMENT aGiorno (#PCDATA)>
<!ELEMENT Orario (#PCDATA)>

<!ELEMENT MaxRisposte (#PCDATA)>
```

– **Descrizione dei campi:**

Obb.	Nome	Tipo	Lung.	Descrizione	Valore	HL7 2.3.1 compliance
SI	idCup	N	9	Identificativo del sistema che effettua la richiesta		MSH.3
SI	idOperatore	AN	20	Identificativo dell’operatore che effettua la richiesta		MSH.4
SI	DataOra	N	12	La data e l’ora della richiesta	Formato: AAAAMMGGHHMI	MSH.7
NO	tipoEsenzione	AN	1	Identificativo dell’esenzione dell’assistito (significativo nel SSN)	Totale = “T” Parziale = “P” Nessuna = “N”	PV1.2
NO	Sesso	AN	1	Identifica il sesso dell’assistito	Maschio=“M” Femmina=“F”	PID.8
NO	DataNascita	N	8	Data di nascita dell’assistito	Formato: AAAAMMGG	PID.7
NO	Urgenza	AN	1	Indica il grado di priorità della richiesta	Urgente=“U” Normale=“N” ---------- Livello 2 (<=24h) Livello 3 (<=7gg) Livello 4 (prog.)	PV1.4
SI	idPrestazione	N	12	Identificativo della prestazione da prenotare		AIS.3.CE.1
NO	idStruttura	N	12	Identificativo della struttura erogante preferita		AIL.4.CE.1
NO	idUnitàErogante	N	12	Identificativo della Unità Erogante preferita		AIL.5.CE.1
NO	daGiorno	N	8	Data a partire dalla quale si cerca l’appuntamento	Formato: AAAAMMGG	ARQ.11.DR.2
NO	aGiorno	N	8	Data fino alla quale si cerca l’appuntamento	Formato: AAAAMMGG	ARQ.11.DR.2
NO	Orario	N	4	Orario intorno al quale cercare l’appuntamento	Formato: HHMI	APR.1.SCV.2 configurando: APR.1.SCV.1=PREFSTART
NO	MaxRisposte	N	2	Specifica il numero massimo di proposte che vengono richieste		QRD.7.CQ.1 configurando: QRD.7.CQ.2=RD

Risposta Disponibilità

– **DTD:**

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT RISPOSTA_DISPONIBILITA (PRESTAZIONE, APPUNTAMENTI*)>
<!ATTLIST RISPOSTA_DISPONIBILITA
   idCUP ID #REQUIRED
   DataOra CDATA #REQUIRED
>

<!ELEMENT PRESTAZIONE (idPrestazione, Denominazione, AvvertenzeOperatore?,
PreparazioneUtente?)>
<!ELEMENT idPrestazione (#PCDATA)>
<!ELEMENT Denominazione (#PCDATA)>
<!ELEMENT AvvertenzeOperatore (#PCDATA)>
<!ELEMENT PreparazioneUtente (#PCDATA)>
```

```
<!ELEMENT APPUNTAMENTI (idAppuntamento, STRUTTURA, UNITA_EROGANTE,
DataOraApp)>
<!ELEMENT idAppuntamento (#PCDATA)>

<!ELEMENT STRUTTURA (idStruttura, DenominazioneST)>
<!ELEMENT idStruttura (#PCDATA)>
<!ELEMENT DenominazioneST (#PCDATA)>

<!ELEMENT UNITA_EROGANTE (idUnitaErogante, DenominazioneUE)>
<!ELEMENT idUnitaErogante (#PCDATA)>
<!ELEMENT DenominazioneUE (#PCDATA)>

<!ELEMENT DataOraApp (#PCDATA)>
```

– **Descrizione dei campi**

Obb.	Nome	Tipo	Lung.	Descrizione	Valore	HL7 2.3.1 compliance
SI	idCup	N	9	Identificativo del sistema che risponde alla richiesta		MSH.3
SI	DataOra	N	12	La data e l’ora della risposta	Formato: AAAAMMGGHHMI	MSH.7
SI	idPrestazione	N	12	Identificativo della prestazione richiesta		AIS.3.CE.1
SI	Denominazione	AN	80	Denominazione della prestazione		AIS.3.CE.2
NO	AvvertenzeOperatore	AN	300	Avvertenze destinate all’operatore		NTE.3 configurando*: NTE.1=1
NO	PreparazioneUtente	AN	300	Preparazione e/o Istruzioni da comunicare all’assistito		NTE.3 configurando*: NTE.1=2
SI	idAppuntamento	AN	12	Identificativo assegnato alla proposta di appuntamento		SCH.5.CE.1
SI	idStruttura	N	12	Identificativo della struttura erogante la proposta		AIL.4.CE.1
SI	DenominazioneST	AN	80	Denominazione della struttura proposta		AIL.4.CE.2
SI	idUnitàErogante	N	12	Identificativo della Unità Erogante la proposta		AIL.5.CE.1
SI	DenominazioneUE	AN	80	Denominazione della Unità Erogante proposta		AIL.5.CE.2
SI	DataOraApp	N	12	Data e ora proposta per l’appuntamento	Formato: AAAAMMGGHHMI	AIL.6

* n.b.: I valori 1 (per avvertenze operatore) e 2 (per istruzioni utente) sono solo di esempio, poiché essi devono essere definiti in maniera generale nel sistema.

Richiesta di prenotazione

– **DTD**

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT RICHIESTA_PRENOTAZIONE (ASSISTITO, PRESTAZIONE, APPUNTAMENTO,
PRESRIZIONE?)>
<!ATTLIST RICHIESTA_PRESTAZIONE
   idCUP ID #REQUIRED
   idOperatore ID #REQUIRED
   DataOra CDATA #REQUIRED
```

```
>

<!ELEMENT ASSISTITO (CodSanitario?, CodFiscale, Nome, Cognome, Sesso, DataNascita)>
<!ELEMENT CodSanitario (#PCDATA)>
<!ELEMENT CodFiscale (#PCDATA)>
<!ELEMENT Nome (#PCDATA)>
<!ELEMENT Cognome (#PCDATA)>
<!ELEMENT Sesso (#PCDATA)>
<!ELEMENT DataNascita (#PCDATA)>

<!ELEMENT PRESTAZIONE (IdPrestazione, Denominazione, AvvertenzeOperatore?,
PreparazioneUtente?)>
<!ELEMENT IdPrestazione (#PCDATA)>
<!ELEMENT Denominazione (#PCDATA)>
<!ELEMENT AvvertenzeOperatore (#PCDATA)>
<!ELEMENT PreparazioneUtente (#PCDATA)>

<!ELEMENT APPUNTAMENTO (IdAppuntamento, STRUTTURA, UNITA_EROGANTE,
DataOraApp)>
<!ELEMENT IdAppuntamento (#PCDATA)>
<!ELEMENT DataOraApp (#PCDATA)>

<!ELEMENT STRUTTURA (idStruttura, DenominazioneST)>
<!ELEMENT idStruttura (#PCDATA)>
<!ELEMENT DenominazioneST (#PCDATA)>

<!ELEMENT UNITA_EROGANTE (idUnitaErogante, DenominazioneUE)>
<!ELEMENT idUnitaErogante (#PCDATA)>
<!ELEMENT DenominazioneUE (#PCDATA)>

<!ELEMENT PRESCRIZIONE (TipoImpegnativa?, IdImpegnativa?, DataPrescrizione?,
NotaPrescrizione?, Urgenza?, IdEsenzione?, IdPrescrittore?)>
<!ELEMENT TipoImpegnativa (#PCDATA)>
<!ELEMENT IdImpegnativa (#PCDATA)>
<!ELEMENT DataPrescrizione (#PCDATA)>
<!ELEMENT NotaPrescrizione (#PCDATA)>
<!ELEMENT Urgenza (#PCDATA)>
<!ELEMENT IdEsenzione (#PCDATA)>
<!ELEMENT IdPrescrittore (#PCDATA)>
```

– Descrizione dei campi

Obb.	Nome	Tipo	Lung.	Descrizione	Valore	HL7 2.3.1 compliance
SI	idCup	N	9	Identificativo del sistema che effettua la richiesta		MSH.3
SI	idOperatore	AN	20	Identificativo dell’operatore che effettua la richiesta		MSH.4
SI	DataOra	N	12	La data e l’ora della richiesta	Formato: AAAAMMGGHHMI	MSH.7
NO	CodSanitario	AN	16	Codice Sanitario dell’assistito		PID.2
SI	CodFiscale	AN	16	Codice Fiscale dell’assistito		PID.4
SI	Nome	AN	48	Nome dell’assistito		PID.5.XPN.1
SI	Cognome	AN	48	Cognome dell’assistito		PID.5.XPN.2
SI	Sesso	AN	1	Sesso dell’assistito	Maschio=“M” Femmina=“F”	PID.8
SI	DataNascita	N	8	Data di nascita dell’assistito	Formato: AAAAMMGG	PID.7
SI	idPrestazione	N	12	Identificativo della prestazione da prenotare		AIS.3.CE.1
SI	Denominazione	AN	80	Denominazione della prestazione		AIS.3.CE.2
NO	AvvertenzeOperatore	AN	300	Avvertenze destinate all’operatore		NTE.3 configurando*: NTE.1=1
NO	PreparazioneUtente	AN	300	Preparazione da		NTE.3

				comunicare all’assistito		configurando*: NTE.1=2
SI	idAppuntamento	AN	12	Identificativo assegnato alla proposta di appuntamento		ARQ.5.CE.1
SI	idStruttura	N	12	Identificativo della struttura		AIL.4.CE.1
SI	DenominazioneST	AN	80	Denominazione della struttura		AIL.4.CE.2
SI	idUnitaErogante	N	12	Identificativo della Unità Erogante		AIL.5.CE.1
SI	DenominazioneUE	AN	80	Denominazione della Unità Erogante		AIL.5.CE.2
SI	DataOraApp	N	12	Data e ora dell’appuntamento	Formato: AAAAMMGGHHMI	ARQ.11.DR.1 e ARQ.11.DR.2**
NO	TipoImpegnativa	AN	3	Indica se si tratta di un’impegnativa compilata dal Medico generico o altri casi		PV1.5.CX.5
NO	IdImpegnativa	N	16	Identificativo dell’impegnativa		PV1.5.CX.1
NO	DataPrescrizione	N	8	Data di emissione della prescrizione/impegnativa	Formato: AAAAMMGG	PV1.25
NO	NotaPrescrizione	AN	300			NTE.3 configurando*: NTE.1=3
NO	Urgenza	AN	3	Indica il grado di priorità della richiesta	Urgente=”U” Normale=”N”	PV1.4
NO	IdEsenzione	AN	1	Identificativo dell’esenzione (identificativo del caso SSN)		PV1.2
NO	IdPrescrittore	N	16	Codice identificativo del medico prescrivente		STF.2

* n.b.: I valori 1 (per avvertenze operatore), 2 (per istruzioni utente) e 3 (note impegnativa) sono solo di esempio, poiché essi devono essere definiti in maniera generale nel sistema.

**n.b.: abbiamo riportato due elementi del protocollo HL7, poiché in esso, occorre assumere il vincolo che essi siano uguali nei valori per effettuare una specifica prenotazioni.

Risposta di prenotazione

– DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT RISPOSTA_PRENOTAZIONE (ASSISTITO, PRENOTAZIONE, PRESCRIZIONE?,
APPUNTAMENTO, CORRISPETTIVO)>
<!ATTLIST RICHIESTA_PRESTAZIONE
   idCUP ID #REQUIRED
   DataOra CDATA #REQUIRED
>

<!ELEMENT ASSISTITO (CodSanitario?, CodFiscale)>
<!ELEMENT CodSanitario (#PCDATA)>
<!ELEMENT CodFiscale (#PCDATA)>

<!ELEMENT PRENOTAZIONE (idPrenotazione, idPrestazione, Denominazione,
AvvertenzeOperatore?, PreparazioneUtente?)>
<!ELEMENT IdPrenotazione (#PCDATA)>
<!ELEMENT IdPrestazione (#PCDATA)>
<!ELEMENT Denominazione (#PCDATA)>
<!ELEMENT AvvertenzeOperatore (#PCDATA)>
<!ELEMENT PreparazioneUtente (#PCDATA)>

<!ELEMENT PRESCRIZIONE (TipoImpegnativa?, IdImpegnativa?)>
<!ELEMENT TipoImpegnativa (#PCDATA)>
<!ELEMENT IdImpegnativa (#PCDATA)>
```

<!ELEMENT APPUNTAMENTO (IdAppuntamento, STRUTTURA, UNITA_EROGANTE, DataOraApp)>
<!ELEMENT IdAppuntamento (#PCDATA)>
<!ELEMENT DataOraApp (#PCDATA)>

<!ELEMENT STRUTTURA (idStruttura, DenominazioneST)>
<!ELEMENT idStruttura (#PCDATA)>
<!ELEMENT DenominazioneST (#PCDATA)>

<!ELEMENT UNITA_EROGANTE (idUnitaErogante, DenominazioneUE)>
<!ELEMENT idUnitaErogante (#PCDATA)>
<!ELEMENT DenominazioneUE (#PCDATA)>

<!ELEMENT CORRISPETTIVO (Euro)>
<!ELEMENT Euro (#PCDATA)>

– Descrizione dei campi

Obb.	Nome	Tipo	Lung.	Descrizione	Valore	HL7 2.3.1 compliance
SI	idCup	N	9	Identificativo del sistema che risponde		MSH.3
SI	DataOra	N	12	La data e l’ora della risposta	Formato: AAAAMMGGHHMI	MSH.7
NO	CodSanitario	AN	16	Codice Sanitario dell’assistito		PID.2
SI	CodFiscale	AN	16	Codice Fiscale dell’assistito		PID.4
SI	idPrenotazione	N	12	Identificativo dal sistema per l’intera richiesta di prenotazione		SCH.2.EI.3
SI	idPrestazione	N	12	Identificativo della prestazione da prenotare		AIS.3.CE.1
SI	Denominazione	AN	80	Denominazione della prestazione		AIS.3.CE.2
NO	AvvertenzeOperatore	AN	300	Avvertenze destinate all’operatore		NTE.3 configurando*: NTE.1=1
NO	PreparazioneUtente	AN	300	Preparazione da comunicare all’assistito		NTE.3 configurando*: NTE.1=2
SI	idAppuntamento	AN	12	Identificativo assegnato all’ appuntamento		SCH.5.CE.1
SI	idStruttura	N	12	Identificativo della struttura erogante		AIL.4.CE.1
SI	DenominazioneST	AN	80	Denominazione della struttura		AIL.4.CE.2
SI	idUnitaErogante	N	12	Identificativo della Unità Erogante		AIL.5.CE.1
SI	DenominazioneUE	AN	80	Denominazione della Unità Erogante		AIL.5.CE.2
SI	DataOraApp	N	12	Data e ora dell’appuntamento	Formato: AAAAMMGGHHMI	SCH.11.TQ.4 e SCH.11.TQ.5**
NO	TipoImpegnativa	AN	3	Indica se si tratta di un’impegnativa compilata dal Medico generico o altri casi		PV1.5.CX.5
NO	IdImpegnativa	N	16	Identificativo dell’impegnativa		PV1.5.CX.1
SI	Euro	N	8	Importo della prestazione	Formato: EEEEEECC	PV1.49

* n.b.: I valori 1 (per avvertenze operatore), 2 (per istruzioni utente) e 3 (note impegnativa) sono solo di esempio, poiché essi devono essere definiti in maniera generale nel sistema.
** n.b.: abbiamo riportato due elementi del protocollo HL7, poiché in esso, occorre assumere il vincolo che essi siano uguali nei valori per effettuare una specifica prenotazioni.

Un esempio di interfacce WEB ipotizzate per la procedura in esame sono riportate nelle seguenti figure, per esse valgono considerazioni analoghe a quelle date per la procedura di “Consultazione Anagrafe Assistiti”.

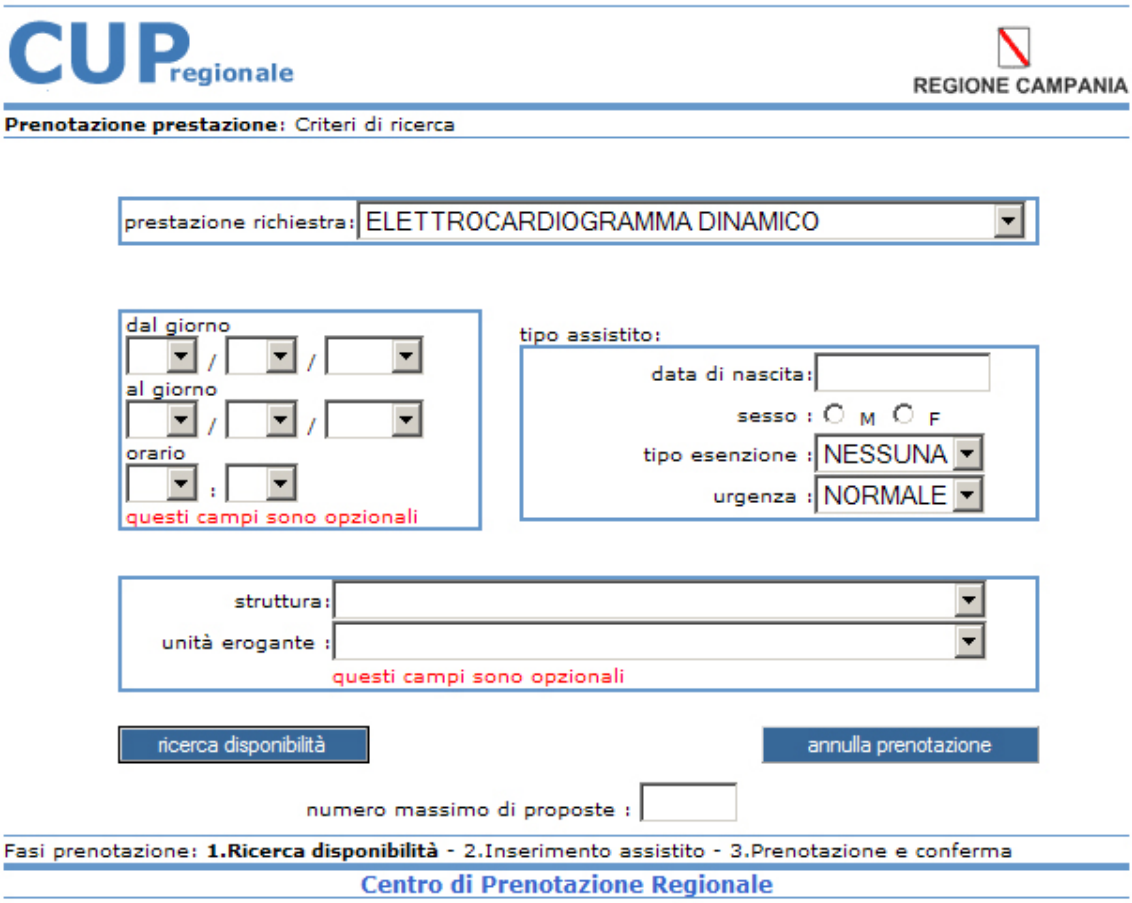


Figura 3 - inserimento criteri di ricerca

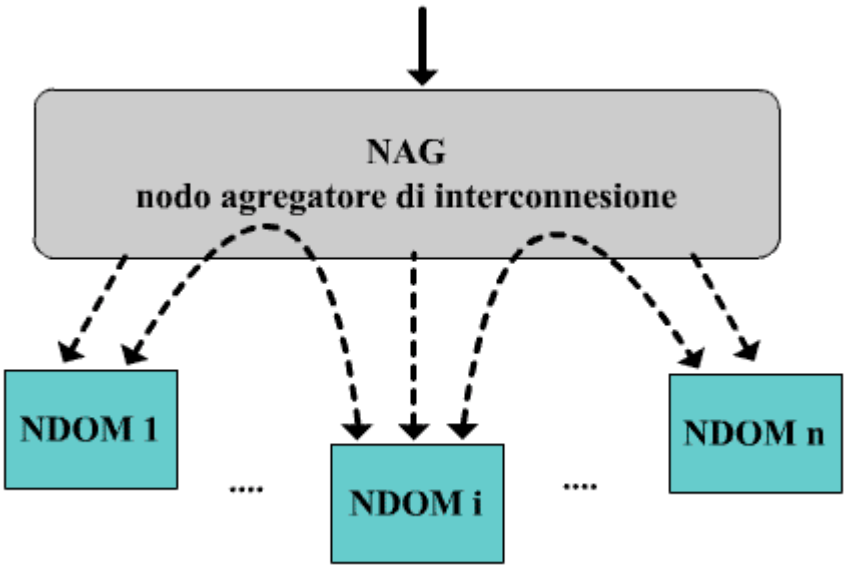
In particolare, essa rappresenta il primo passo per la procedura di “Prenotazione Prestazione”. Attraverso essa, l’utente potrà inserire i criteri di ricerca per determinare la disponibilità, da parte dell’ente consultato, ad erogare una specifica prestazione in base alle preferenze dell’assistito. Tale preferenze, non obbligatorie, sono relative a dimensioni temporali (fascia oraria, giorno di preferenza…) e a una dimensione spaziale (struttura erogatrice…).

5.3 Esempio di funzionamento: accesso a servizi non disponibili su un nodo di dominio

Il modello cooperativo potrà funzionare in due diverse modalità tramite:

- Un utente accede al nodo aggregatore che seleziona tra più risorse quella di interesse;
- una interazione tra nodi di dominio. In questo caso, all’atto della richiesta di un servizio, un nodo di dominio, se non è in grado di far fronte alla richiesta, può inoltrarla ad un altro nodo di dominio presso un altro Ente in maniera completamente trasparente all’utente. Ad esempio per una richiesta di prenotazione di una prestazione sanitaria, è possibile che un

nodo che non ha più disponibilità possa automaticamente inoltrare la richiesta ad un altro nodo erogatore (figura).



Quando un utente tramite il NAG o un nodo di dominio inoltra una richiesta di servizio, il funzionamento del sistema prevede di:

- Identificare e autenticare l’utente (autenticazione debole o forte), verifica le sue autorizzazioni per quell’Ente;
- Determinare, in base alla tipologia di servizio richiesto, gli Enti esterni che può coinvolgere per inoltrare la richiesta;
- Inviare la richiesta ad un altro Ente sfruttando il collegamento del nodo erogatore;
- Attendere la risposta;
- Determinare il servizio che può effettuare;
- Inviare all’Ente prescelto la richiesta di servizio;
- Attendere conferma dell’avvenuta esecuzione del servizio;
- Registrare in un proprio archivio che il servizio per quell’utente è stato offerto mediante richiesta ad un Ente esterno.

Specularmene, il Nodo di dominio che è disponibile ad erogare il servizio:

- Riceve la richiesta grazie al collegamento con il nodo aggregatore.
- Controlla la disponibilità ad erogare il servizio,
- Risponde, in caso affermativo, con la sua disponibilità ad erogare il servizio
- Riceve la richiesta e invia la conferma se il servizio è ancora disponibile o, in caso contrario, (servizio non più disponibile) invia la sua indisponibilità.

5.4 Componenti fisici per il NAG del CUP

Si fa esplicitamente notare che:

- le funzioni base del Nodo Aggregatore e le funzioni specifiche relative al sistema CUP devono essere realizzate in due architetture fisicamente distinte, che possano essere allocate in due diversi punti di accesso della rete della Regione Campania;

- le componenti, o istanze delle componenti, che implementano le funzioni base del NAG possono essere utilizzate, in modo totale o parziale, anche per la realizzazione del sistema CUP, laddove la Ditta fornitrice lo ritenga necessario per la realizzazione dell’applicazione.

Il sistema per la realizzazione del CUP deve tuttavia avere almeno i seguenti sistemi:

- un sistema per lo sviluppo delle applicazioni di integrazione e cooperazione dei sistemi CUP, strutturato mediante un’architettura a tre livelli (presentazione, applicazione, data base);
- un sistema di autenticazione locale di secondo livello, eventualmente attivabile se è previsto un ulteriore livello di autenticazione rispetto a quello previsto per le funzionalità di base del nodo di aggregazione. Tale sistema è specifico per l’accesso i servizi del dominio e deve operare in modo integrabile con i meccanismi di autenticazione ed autorizzazione del nodo CUP e in modo conforme a quanto visto negli scenari applicativi;
- un sistema per il monitoraggio e la tracciabilità specifico e unicamente relativo all’applicazione in esame che consente di monitorare le richieste verso i diversi Enti che offrono i servizi di prenotazione. Tale sistema deve essere utilizzabile in modo autonomo da operatori preposti al controllo dell’applicazione e deve essere integrabile con quello previsto dal NAG. Per gli eventi da monitorare si può fare riferimento alla descrizione delle componenti sulla tracciabilità e monitoraggio. Il controllo deve essere esteso anche a funzionalità che premettono di analizzare gli Enti attivi nella rete.
- un sistema per la gestione della “sicurezza fisica” già descritte nel paragrafo sulla sicurezza perimetrale del NAG;
- un sistema per la gestione dei dati che include la archiviazione, sistemi di back-up e di mirroring.
- 10 postazioni client per l’accesso alla piattaforma dotati di dispositivi di utilità per l’utilizzo dei servizi CUP, quali dispositivi e lettori di smartcard;
- Un sistema di stampa (almeno un server di stampa e 2 stampanti ad elevata risoluzione).

- Devono essere opportunamente previsti apparati di rete (layer 2 e 3) che permettano la realizzazione di una infrastruttura di rete a larga banda per la interconnessione delle componenti di sicurezza e per l’integrazione con piena compatibilità della piattaforma nella intranet regionale:
    - Router
    - Switch
    - Access Point
    - Terminale di configurazione-controllo

- Armadi rack

- Gruppi di continuità

Laddove fossero necessarie ulteriori componenti o la replicazione di componenti presenti nel nodo NAG per la realizzazione delle funzioni base, l’Impresa si può riservare di utilizzare ulteriori sistemi o di allocare opportunamente le nuove componenti su uno dei sistemi già previsti non pregiudicandone prestazioni e funzionalità.

Tutti i sistemi, fatta eccezione per le postazioni client, devono essere composti almeno da 2 nodi bi-processore al fine di garantire opportune caratteristiche prestazionali e di affidabilità grazie alla ridondanza dei componenti architetturali. Al pari di quanto previsto per il sistema che implementa le funzioni base del NAG ogni miglioramento all’architettura, fatto per incrementare prestazioni ed affidabilità, basato sull’incremento di unità funzionali, può essere considerato.

6 Valutazione dell’architettura e livelli di servizio del sistema

La fornitura del sistema, sia per le funzionalità base del nodo NAG che per quelle specifiche del CUP, nelle sue componenti Hardware e Software, e nella progettazione del sistema, deve essere dimensionata e commisurata alle aspettative esposte di seguito in termini di qualità, prestazione e di soddisfazione dei livelli di servizio.

L’Impresa fornitrice si impegna ad assicurare in relazione alle diverse tipologie e tenuto conto del rilievo a livello pubblico delle servizi erogati dalla Regione Campania, un alto standard nei livelli di servizio (SLA – Service Level Agreement) del sistema; per fornire alcuni degli elementi di valutazione oltre a quanto definito nel Capitolato Speciale, nella fornitura è almeno necessario evidenziare:

1. la qualità e le prestazione dei componenti Hardware,
2. la qualità dei componenti Software,
3. i livelli di qualità dichiarati per accedere alle funzionalità offerte dai singoli servizi.

In particolare, il terzo elemento di valutazione è stato introdotto per tener conto di una valutazione quantitativa e qualitativa sulle funzionalità che il sistema deve, nel suo complesso, presentare; le valutazioni devono essere fornite con riferimento puntuale a quanto indicato nei seguenti paragrafi.

6.1 Valutazione dell’ Hardware

Al fine di garantire lo sviluppo in qualità di tutti gli elementi che caratterizzano la fornitura, l’impresa, in fase di gara, dovrà presentare la documentazione per descrivere, in modo puntuale, l’architettura di tutti gli elementi hardware che intende utilizzare per la progettazione del sistema (nodi di elaborazione, apparati di rete, etc…).
Le prestazioni dei componenti hardware che costituiscono il sistema rappresentano un punto decisivo per la valutazione della fornitura e saranno valutate in termini di potenza elaborativa, dei dispositivi di I/O, delle prestazioni di rete (collegamento tra le diverse unità), delle soluzioni adottate, della flessibilità, modularità e manutenibilità del sistema stesso.

6.2 Valutazione del software

Al fine di garantire lo sviluppo in qualità di tutti gli elementi che caratterizzano la fornitura, l’impresa, in fase di gara, dovrà presentare la documentazione per descrivere l’architettura dei moduli software e il ciclo di sviluppo per tutti i moduli che intende realizzare specificamente per il progetto. In fase di realizzazione, l’azienda si impegna a fornire, secondo un formato concordato con la Regione Campania, la documentazione relativa ai moduli, oggetto della realizzazione (UML dei componenti, delle API, della classi, della struttura dei DB, etc..) sia per quanto riguarda le funzionalità offerte all’utente finale che per garantire che sia possibile sviluppare applicazioni usufruendo dei moduli realizzati, e si impegna a fornire il piano dei test.
Per i moduli software di base acquisiti da terze parti, dovrà essere fornita una descrizione sulle funzionalità e sulle prestazioni, così come rilevate in casi d’uso tipici.

6.3 Livelli di servizio

L’Impresa fornitrice si impegna ad assicurare in relazione alle diverse tipologie e tenuto conto del rilievo a livello pubblico dei servizi erogati dalla Regione Campania, un alto standard nei livelli di servizio (SLA – Service Level Agreement).
I livelli di servizio che dovranno essere assicurati, in particolare, riguardano i seguenti campi di intervento:

- servizi Web (erogazione servizi Web Services e servizi base);
- servizi per l’integrazione e l’interoperabilità;
- servizi di sicurezza;
- manutenzione del sistema.

Si fa esplicitamente notare che per i servizi elementari del CUP che dipendono dai nodi di dominio (AASSLL e AAOO), come descritto nei precedenti paragrafi, la ditta fornitrice avrà solo il compito di tracciare e monitorare la richiesta di servizio e i tempi di risposta.

6.4 Elementi generali dei livelli di servizio attesi

Obiettivo di tale paragrafo è definire le specifiche ed i requisiti che il sistema deve presentare e che devono essere valutati in fase di gara e di realizzazione al fine di garantire un alto standard di qualità della fornitura in termini di affidabilità, intesa come capacità del servizio di mantenere attivo il suo funzionamento e la qualità di erogazione del servizio stesso, e di qualità della fornitura.
Tutti i valori di soglia definiti per ogni SLA sono da intendersi come requisiti minimali richiesti dal sistema, anche ove non esplicitamente evidenziato.
La qualità della fornitura dovrà essere assicurata dall’Impresa fornitrice attraverso:

- l’applicazione del Piano della sicurezza, del Piano della Qualità e del Piano di manutenzione, definiti di seguito, che devono essere prodotti in fase di gara in quanto oggetto di valutazione;
- il soddisfacimento dei parametri definiti per i livelli di servizio;
- il monitoraggio del rispetto dei livelli di servizio e l’attivazione di eventuali azioni correttive a fronte del mancato rispetto.

La rilevazione dei livelli di servizio sarà contestuale all’inizio dell’esercizio dell’infrastruttura.

6.5 Piano per la sicurezza

Per valutare la progettazione dell’architettura di sicurezza, in fase di gara devono essere presentati i seguenti documenti:

- documento di Risk Assesment;
- documento di Risk Management;
- documento con il Piano della Sicurezza

Risk Assessment
La progettazione del sistema di sicurezza deve avere come premessa vincolante un processo di Risk Assessment del sistema, che deve fornire un documento il cui contenuto deve chiaramente esporre:

- Classificazione degli asset critici del sistema.
- Classificazione e valutazione delle minacce.
- Classificazione e valutazione delle vulnerabilità del sistema.
- Valutazione dell’impatto dei vari rischi sul sistema.
- Analisi dei risultati.

Risk Management
A valle del processo di Risk Assessment, deve seguire una fase ulteriore in cui i risultati di tale processo devono fornire la base di partenza per operazioni di contenimento dei rischi e diventare specifiche vincolanti per la progettazione dell’architettura di sicurezza definitiva.

- Identificazione e classificazione dei rischi come risultati del Risk assessment.
- Modalità di controllo dei rischi identificati.
- Modalità di minimizzazione o rimozione dei rischi.
- Valutazione dell’impatto sul sistema in termini di complessità d’uso.
- Definizione delle procedure di intervento e delle azioni correttive da intraprendere al presentarsi dei rischi valutati.
- Piani di auditing periodici.
- Piani di Business Continuità Planning (BCP) e Disaster Recovery

Piano della sicurezza
Risultato dei due precedenti processi deve essere la stesura di un documento che si basa sull’analisi del sistema svolta e fornisce le specifiche dettagliate dell’architettura di sicurezza da realizzare.
In particolare occorrerà indicare le politiche per il controllo degli accessi che verranno poi personalizzate dagli amministratori di sistema, in funzione dei ruoli che gli utenti possono assumere e delle risorse che l’architettura presenta.
Tale documento deve essere pubblicato, approvato e comunicato ad ogni interessato, potrà essere inoltre modificato successivamente se si dovessero verificare esigenze differenti da parte della Regione Campania.

6.6 Piano della qualità

Il Piano della Qualità definisce le caratteristiche qualitative cui deve sottostare l’intera fornitura. L’Impresa fornitrice dovrà rendere disponibili alla Regione Campania in fase di gara una descrizione delle metodologie che intende adoperare per garantire la qualità del processo di produzione, del *Piano della Qualità*, delle procedure di sistema e della documentazione di gestione che intende seguire per lo svolgimento del progetto e per la sua successiva gestione. In occasione della realizzazione tale piano deve essere fornito in modo dettagliato e deve essere accettato dalla Regione.
La Regione Campania si riserva la facoltà di richiedere, ogni volta che lo reputi opportuno, una nuova versione o revisione del Piano della Qualità.

Nella redazione del piano, il fornitore dovrà tenere come guida lo schema di riferimento di seguito descritto:

1. Scopo del Piano della Qualità (contiene lo scopo del piano della qualità ed una sintesi dei suoi contenuti).

2. Documenti di Riferimento (contiene l'elenco dei documenti di riferimento al piano della qualità).
3. Glossario (contiene le abbreviazioni, gli acronimi, le definizioni, che saranno utilizzati all’interno del documento).
4. Gestione:
   4.1 Organigramma ed Interfacce (contiene l'organigramma della fornitura con l'identificazione dei responsabili delle varie attività della fornitura, del responsabile dei controlli da svolgere, del responsabile della gestione della configurazione, del responsabile della gestione delle non conformità e le relazioni con le altre organizzazioni coinvolte nella fornitura)
   4.2 Ruoli e Responsabilità (contiene le responsabilità di ciascun ruolo definito nell'organigramma della fornitura. Utilizzare una matrice, denominata “matrice delle responsabilità”, per sintetizzare le responsabilità assegnate)

5. Obiettivi di qualità :
   5.1 Requisiti di qualità dell’intera fornitura (contiene gli attributi della qualità relativi a ciascun servizio (caratteristiche e sottocaratteristiche), le metriche con cui misurare gli attributi, i valori limite delle metriche ritenuti accettabili (valori di soglia))
   5.2 Procedura di valutazione della qualità (contiene la procedura di valutazione della qualità dei prodotti e dei servizi)
6. Riesami, Verifiche e Validazione (contiene l'indicazione della tipologia di controlli (riesami, verifiche, validazioni) da effettuare, degli strumenti da utilizzare per i controlli, la modulistica di rendicontazione dei risultati per tutte le attività di fornitura e la modulistica per la rilevazione della soddisfazione della Regione Campania).
7. Segnalazione di Problemi ed Azioni Correttive (contiene le modalità di gestione di problemi, il tracciamento e la risoluzione delle non conformità e delle azioni correttive).
8. Strumenti, Tecniche e Metodi (contiene l'indicazione delle metodologie, degli standard dei deliverable, degli standard di utilizzo di prodotti per le attività di erogazione dei servizi e di produzione della documentazione).
9. Formazione ed Addestramento compresa nei servizi di base (contiene la descrizione delle attività di formazione e di addestramento).
10. Analisi e dati per il miglioramento (contiene le modalità di rilevazione, analisi e rendicontazione dei dati per le attività legate al miglioramento dei servizi).

Il Piano della Qualità deve essere prodotto in fase di gara, il Piano della Qualità Generale dovrà essere consegnato entro 20 giorni lavorativi dall’inizio delle attività della fornitura.

La Regione Campania si riserva 30 giorni dalla consegna per l’approvazione del Piano della Qualità Generale. L’approvazione del Piano della Qualità Generale, come pure gli eventuali rilievi, verranno formalizzati per iscritto, assegnando inoltre il termine per la consegna del Piano modificato.
Il Piano della Qualità Generale non prevede approvazione per tacito assenso.

Le variazioni sui contenuti dei Piani della Qualità Generale dovranno essere consegnate entro 10 giorni lavorativi dalla formalizzazione dei rilievi.

6.7 Piano di Manutenzione

Va sviluppato un piano per definire gli interventi oggetto di manutenzione con una valutazione temporale degli interventi previsti. In particolare, in sede di gara, va prevista:

- **La manutenzione preventiva,** che consiste in interventi, concordati con la Regione Campania, (regolazioni, controlli, sostituzioni) da effettuare periodicamente al fine di consentire la perfetta funzionalità del sistema e prevenirne i malfunzionamenti;
- **la manutenzione correttiva,** che consiste sia nella riparazione dei guasti, bloccaggio o altro inconveniente che dovesse verificarsi, sia nella messa a disposizione di tutte le parti di ricambio in sostituzione e nell’esecuzione delle prove e dei controlli necessari a garantire il ripristino del pieno funzionamento del sistema;
- **la manutenzione evolutiva,** che consiste sia nella allineamento dell’hardware e del firmware dei prodotti alle ultime release previste dal costruttore, nonché all’ eventuale allineamento dei medesimi alle modifiche eventualmente richieste dai sistemi operativi. Nella manutenzione evolutiva vanno considerati senza oneri tutti gli adeguamenti che saranno necessari per recepire le normative e direttive secondo quanto riportato in premessa.

Per tutti i tipi di manutenzione sopra indicati, l’Impresa dovrà utilizzare parti di ricambio di primaria qualità con elementi nuovi di fabbrica, prodotte dallo stesso costruttore. Il servizio comprenderà altresì, a totale carico dell’Impresa fornitrice, l’effettuazione delle modifiche tecniche, consistenti nei miglioramenti e/o aggiornamenti, al fine di elevare il grado di affidabilità del sistema, di migliorare il funzionamento e di aumentare la sicurezza.

6.8 Valutazione dei livelli di servizio

Per la valutazione dei livelli di servizio, l’Impresa fornitrice dovrà rilevare i parametri riportati nei paragrafi seguenti, compresi quelli non utilizzati direttamente per la valutazione delle penali.
La valutazione dei livelli di servizio e' fatta su base quadrimestrale pertanto i parametri rilevati dovranno rimanere nei limiti indicati nel quadrimestre di riferimento.
Occorre sottolineare che, laddove è presente un valore numerico dei parametri, questo è da intendersi come valore minimo atteso dalla Regione Campania (valore di soglia).
Il mancato rispetto di tali livelli comporterà, ove previsto, l’applicazioni delle penali riportate nel contratto.

6.8.1 Definizioni analitiche dei parametri

Si intende come:

Finestra temporale di erogazione	Arco di tempo su cui vengono calcolati i livelli di servizio, assunto pari all’orario di erogazione dei servizi.
Periodo di osservazione contrattuale	Arco di tempo, individuato in quattro mesi, entro il quale devono essere rispettati i livelli di servizio: il primo decorre due mesi dopo l’inizio dell’attività di gestione

Disponibilità	percentuale di tempo durante il quale il singolo servizio è funzionante (ovvero non vi é interruzione di servizio) rispetto alla finestra di erogazione temporale del servizio stesso. Con disponibilità di un servizio, in un determinato periodo di osservazione, si intende, pertanto, la percentuale calcolata con la formula seguente: $$D = \left(1 - \frac{\sum_{j=1}^{M} dj}{T} \right) 100$$ Ove: D = disponibilità espressa come valore percentuale d_j= durata del generico disservizio j , compresa nella finestra temporale di erogazione M = numero di disservizi verificatisi T = periodo di funzionamento del servizio di cui si misura la disponibilità
Disponibilità reale	la disponibilità di cui sopra calcolata comprendendo qualunque interruzione di qualunque natura.
Disponibilità contrattuale	disponibilità al netto delle interruzioni non imputabili al Fornitore quali: • guasti e/o interruzioni dipendenti dalla alimentazione elettrica; • eventi eccezionali di origine naturale (nubifragi, terremoti, etc.); • problematiche relative agli apparati installati nel sito individuato dal Fornitore (alimentazione, allagamenti, incendi, guasti hardware e sw che richiedano l’intervento della manutenzione presso il sito, ecc.); • guasti gravi alle linee e/o apparati del gestore pubblico (tranciatura di cavi, lavori straordinari, etc.).
Arrotondamenti	ai fini del calcolo dello scostamento tra le percentuali di disponibilità effettive e quelle contrattuali la prima deve essere arrotondata: • nel caso di aumento o riduzione dello 0,1 % si arrotonda allo 0% per scostamenti compresi tra lo 0,000% e lo 0,049% ed allo 0,1% per scostamenti superiori; • nel caso di aumento o riduzioni dell'1% si arrotonda allo 0% per scostamenti compresi tra lo 0,00 e lo 0,49 ed all'1% per scostamenti superiori.
Tempo di risposta al disservizio	tempo intercorrente tra la segnalazione del disservizio, attivata in modo automatico o da una chiamata all’assistenza telefonica o dalla Regione Campania, e la segnalazione

	all’utente e/o alla Regione Campania della diagnosi di massima e del tempo di ripristino previsto. Misurazione effettuata nella finestra temporale di erogazione del servizio.
Tempo di ripristino	tempo intercorrente tra la segnalazione del disservizio ed il ripristino delle funzionalità oggetto del disservizio. Misurazione effettuata nella finestra temporale di erogazione del servizio.
Tempo di autenticazione	Tempo necessario al sistema per identificare ed autenticare un utente, da un client collegato alla rete locale del NAG.
Tempo di autorizzazione	Tempo necessario al sistema per prelevare le credenziali di un utente ed autorizzarlo in funzione del suo ruolo e delle risorse a cui vuole accedere, da un client collegato alla rete locale del NAG.
Tempo di accesso ad un servizio	Tempo necessario per accedere ad una funzionalità di un servizio base, a valle della fase di autenticazione ed autorizzazione, da un client collegato alla rete locale del NAG o per il solo accesso all’applicazione CUP da un client collegato alla rete locale del CUP
Tempo di ricerca di un servizio	Tempo necessario per ricercare un servizio pubblicato in un registro, da un client collegato alla rete locale del NAG
Tempo di accesso ad una pagina web	Tempo necessario per visualizzare una pagina web residente in un server del NAG da un client collegato alla rete locale del NAG o per visualizzare una pagina residente in un server del CUP da un client collegato alla sua rete locale

Osserviamo che, per non considerare il contributo dovuto ai tempi di comunicazione della intranet regionale o del sistema SPC, le misure di qualità vengono fatte da un client direttamente collegato alla rete locale del NAG e con il carico successivamente definito in termini di utenti connessi contemporaneamente al sistema.
Quindi, il carico è quello reale e il tempo di risposta è controllabile in tutte le componenti.

6.8.2 Finestra temporale di erogazione

Gli orari di erogazione dei servizi, sia del NAG che del CUP (limitatamente alle funzioni di aggregazione oggetto di gara), devono essere sull’arco dell’intero giorno e per l’intera settimana. In termini di ore, l’erogazione è riportata nella seguente tabella:

Tipo di servizio	Orario di disponibilità	Giorni di disponibilità
Servizi Web	24h nel 99% dei casi	7 giorni su 7
Servizi per l’integrazione e l’interoperabilità;	24h nel 99% dei casi	7 giorni su 7
Servizi di sicurezza	24h nel 99% dei casi	7 giorni su 7

I guasti ai servizi di sicurezza in ogni caso non devono essere critici per il sistema; in caso di guasto, il sistema deve rimanere in uno stato sicuro tra quelli previsti nell’analisi dei rischi.

6.8.3 Tempi di risposta per l’accesso ai servizi

I tempi di risposta per l’accesso ai servizi sono definiti in termini di tempo massimo di erogazione della funzionalità da parte del sistema verso un utente che ne fa richiesta.

Per i servizi erogati dal NAG (servizi base o integrazione di servizi applicativi) si devono rispettare le specifiche di qualità, sicurezza, affidabilità e i parametri di funzionamento che saranno di seguito definiti; mentre per i servizi che coinvolgono altri domini, ove la qualità della risposta non dipende dal NAG, è richiesto il rilevamento dei tempi di risposta dei servizi del dominio. Il sistema di monitoraggio deve, inoltre, essere predisposto per utilizzare i parametri sulla qualità del servizio del sistema di comunicazione, ottenuti da sistema di monitoraggio del Sistema Pubblico di Connettività (SPC), per consentire una valutazione più completa della qualità dei servizi aggregati in termini di tempo di risposta complessivo e tempo di risposta della rete di comunicazione.

La percentuale di successo a cui si fa riferimento è relativa al periodo di esercizio fissato.

Parametro da rilevare	**Limite**
Tempo massimo per visualizzare una pagine web	3’’ nel 95% dei casi
Tempo massimo ricerca di un servizio in un registro	3’’ nel 95% dei casi
Tempo massimo autenticazione utente (autenticazione debole)	3’’ nel 95% dei casi
Tempo massimo autorizzazione utente	3’’ nel 95% dei casi
Tempo di accesso alle funzionalità di un servizio base (depurato dell’autenticazione e dei tempi di comunicazione)	3’’ nel 95% dei casi
Tempo massimo di interruzione di erogazione di un servizio (in assenza di guasto che richiede manutenzione)	3’ nel 95% dei casi

Osserviamo esplicitamente che tra i parametri da rilevare e rispettare sono presenti i tempi di accesso alle funzionalità di un servizio base e non il tempo di risposta dello stesso, essendo quest’ultimo funzione della particolare tipologia dei servizi base, così come definita nel Paragrafo 3. Ad esempio nel caso del CUP, il tempo di risposta è solo rilevabile poiché dipende anche dalla velocità di risposta degli Enti esterni collegati.
Per quanto riguarda l’utilizzo di un meccanismo di autenticazione forte, il tempo massimo per l’autenticazione può variare rispetto a quanto detto precedentemente e deve essere dichiarato dalla Impresa in funzione della tecnologia utilizzata.

Osserviamo inoltre che tutti i parametri numerici devono essere considerati come valori di soglia minimi, mentre tutti i parametri definiti in 6.8.1 a cui non corrispondono dei valori numerici verranno valutati in funzione della qualità dei componenti hardware e software coinvolti secondo quanto previsto nel capitolato speciale e nel presente disciplinare tecnico.

Per soddisfare i parametri precedentemente definiti, il progetto deve essere dimensionato e realizzato nei termini delle sue componenti hardware e software, dell’architettura e delle tecnologie, in modo da soddisfare i seguenti requisiti:

- Bacino di utenza supportato del sistema: nell’ordine di 7000 sessioni attive contemporaneamente.
- Previsione incremento utenze da 7000 a 11000 con decadimento delle prestazioni pari al massimo al 20%.

- Decadimento prestazioni del 10 % ad ogni incremento di 1000 utenti a partire da 11000 fino ad un massimo di 14000 sessioni attive.
- Per utenze superiori al numero di 14000 il sistema potrà, a scelta della Regione Campania, rifiutare ulteriori sessioni o non garantire i livelli di servizio definiti.

Sessioni attive	Accessibilità
fino a 7000	Garantita nel100% dei casi
tra 7001 a 11000	Garantita nel 80% dei casi
tra 11001 a 12000	Garantita nel 70% dei casi
tra 12001 a 13000	Garantita nel 60% dei casi
tra 13001 a 14000	Garantita nel 50% dei casi
Oltre le 14000	Livelli di servizio non garantiti

Il sistema dovrà essere opportunamente dimensionato affinché possa, a regime, gestire oltre 250.000 utenti registrati (utenti di Pubbliche Amministrazioni, Enti Privati e cittadini) e oltre 10.000 servizi da pubblicare nei registri.
Per quanto detto sulla scalabilità, il sistema deve garantire la possibilità di gestire un numero maggiore di sessioni attive di utenti e servizi registrati, al crescere delle esigenze della Regione Campania; tale requisito deve essere soddisfatto senza modifiche al Software applicativo e dell'architettura di riferimento utilizzata, aggiungendo o potenziando le componenti che costituiscono il sistema.

6.8.4 Servizi di manutenzione correttiva

Per valutare il livello di servizio della manutenzione correttiva in garanzia relativa ai servizi forniti, devono essere rilevati i seguenti parametri che dovranno rimanere nei limiti indicati nel periodo di riferimento. Le osservazioni di seguito riportate valgono per le funzionalità base del nodo NAG e per quelle specifiche del CUP.
In funzione delle differenti classificazioni dei servizi e del diverso livello si criticità ad essi associato dal processo di Risk Assessment, vengono previsti tre livelli di criticità:

- Strategico
- Medio
- Basso

A questi corrispondono i relativi livelli di servizio contrattuali di seguito riportati:

Manutenzione correttiva : Tempestività di intervento per guasti di livello Strategico	
Elemento di valutazione	Ripristino dai malfunzionamenti sul sistema
Indicatore	Tempestività nella risoluzione malfunzionamenti di livello: Strategico
Metrica	Percentuale di malfunzionamenti di livello Strategico risolti entro 4 ore
Modalità di misura	$x = \frac{a}{b} * 100$ a = Num. Malfunzionamenti di livello Strategico risolti entro 4 ore

	lavorative b = Num. Malfunzionamenti di livello Strategico
Valore di soglia	= 100%
Modalità di rendicontazione	Registrazione puntuale in formato elettronico di tutti gli interventi effettuati con l’indicazione del codice dell’intervento, numero e data/ora di segnalazione a cui si riferisce l’intervento, di data/ora di inizio intervento.
Penali	Secondo quanto espresso nel Capitolato Speciale
Rilevazione	quadrimestrale

Manutenzione correttiva : Tempestività di intervento per guasti di livello Medio	
Elemento di valutazione	Ripristino dai malfunzionamenti sul sistema
Indicatore	Tempestività nella risoluzione malfunzionamenti di livello: Medio
Metrica	Percentuale di malfunzionamenti di livello Medio risolti entro 1 giorno lavorativo
Modalità di misura	$x = \frac{c}{d} * 100$ c = Num. malfunzionamenti di livello Medio risolti entro 1 giorno lavorativo d = Num. malfunzionamenti di livello Medio risolti
Valore di soglia	≥ 98%
Modalità di rendicontazione	Registrazione puntuale in formato elettronico di tutti gli interventi effettuati con l’indicazione del codice dell’intervento, numero e data/ora di segnalazione a cui si riferisce l’intervento, di data/ora di inizio intervento.
Penali	Secondo quanto espresso nel Capitolato Speciale
Rilevazione	quadrimestrale
Manutenzione correttiva : Tempestività di intervento per guasti di livello Bassi	
Elemento di valutazione	Ripristino dai malfunzionamenti sul sistema
Indicatore	Tempestività nella risoluzione malfunzionamenti di livello: Basso
Metrica	Percentuale di malfunzionamenti di livello Basso risolti entro 4 giorni lavorativi
Modalità di misura	$x = \frac{e}{f} * 100$ e = Num. malfunzionamenti di livello Basso risolti entro 4 giorni lavorativi f = Num. malfunzionamenti di livello Basso risolti

Valore di soglia	≥ 95%
Modalità di rendicontazione	Registrazione puntuale in formato elettronico di tutti gli interventi effettuati con l’indicazione del codice dell’intervento, numero e data/ora di segnalazione a cui si riferisce l’intervento, di data/ora di inizio intervento.
Penali	Secondo quanto espresso nel Capitolato Speciale
Rilevazione	quadrimestrale

Per le definizioni non citate si applicano quelle riportate a livello contrattuale.

6.9 Rendicontazione quadrimestrale

LIVELLI DI SERVIZIO	MISURA DA RILEVARE	VALORI DI SOGLIA
Tempestività nella produzione delle relazioni quadrimestrali da sottoporre al vaglio della Struttura di Supervisione	Tempo intercorrente tra la data di scadenza e la effettiva produzione della rendicontazione	entro 2 gg. nel 85% dei casi
Qualità e Completezza delle relazioni quadrimestrali prodotte	Formato, numerazione, confezionamento, intelligibilità, elementi di presentazione, completezza	entro l’85% degli standard fissati

Per le definizioni non citate si applicano quelle riportate a livello contrattuale.

6.10 Penali Contrattuali

Le penali applicate sono definite nel Capitolato Speciale.

7 Supporto alla realizzazione del sistema

7.1 Gestione e Manutenzione del Sistema

L’Impresa Fornitrice dovrà, inoltre, proporre l’infrastruttura hardware e software tale da poter gestire guasti e attività di manutenzione senza interruzioni del servizio; dovrà specificare le componenti hardware e software per la realizzazione di un completo backup e disaster recovery così come previsto nelle procedure di Risk Management; dovrà fornire adeguati strumenti di monitoraggio di servizi e di infrastruttura, inclusi i servizi di allarmistica in tempo reale.
Il software di base dei server dovrà essere fornito con un numero di licenze d’uso adeguato e dovrà essere in grado di sostenere il carico dell’intero sistema garantendo livelli di servizio adeguati alle caratteristiche funzionali delle applicazioni ed alla tipologia e dimensioni

dell’utenza, in termini di tempi di risposta, quantità di dati gestita, scalabilità, affidabilità, continuità del servizio, sicurezza; dovrà inoltre essere conforme a standard de facto o de iure e dovrà essere in grado di interoperare sui sistemi di rete previsti in tale allegato.

La fornitura prevede la conduzione, la manutenzione, sia preventiva che a richiesta, on site, e la garanzia di tutte le componenti del Sistema per 36 mesi a partire dal positivo collaudo finale dell’intero Sistema;

Il fornitore nell’effettuare tutte le attività manutentive sul software e sull’hardware deve garantire la continuità e la qualità dei servizi richiesti. Dovrà, inoltre, provvedere ad effettuare la necessaria manutenzione correttiva ed evolutiva del software applicativo fornito sui client al fine di mantenere tali sistemi aggiornati o di migliorarne le prestazioni.

7.2 Formazione

La fornitura prevede almeno 600 ore di addestramento del personale della Regione Campania che affiancherà il personale della Impresa Fornitrice dell’appalto nella conduzione del sistema; almeno 800 ore di affiancamento del personale della Regione Campania utilizzatore del Sistema.
La formazione sviluppata tramite un apposti piano deve includere la gestione e l’utilizzo del sistema sia per operatori esperti che per utenti finali per quanto attiene:

- l’hardware
- il software commerciale con riferimento alle funzioni necessarie al NAG o all’applicativo CUP
- il software specificamente sviluppato per il NAG o per l’applicativo CUP

La Regione Campania si riserva la possibilità di ripartire diversamente le ore di addestramento e affiancamento, fermo restando le 1400 ore totali.