ASSESSORATO ALL'UNIVERSITA' E
RICERCA SCIENTIFICA, INNOVAZIONE TECNOLOGICA E NUOVA ECONOMIA, SISTEMI INFORMATIVI E STATISTICA

ALLEGATO TECNICO

REQUISITI DEL SISTEMA

Progetto Rete dei Medici di Medicina Generale
(C.U.P. F66J 0300 0090 001; Cod. MEF SI – 02)

Bollettino Ufficiale della Regione Campania n. 63bis del 5 dicembre 2005

INDICE

1 INTRODUZIONE

In questo documento si dettagliano le specifiche dei sistemi e dei servizi che il Fornitore deve sviluppare:

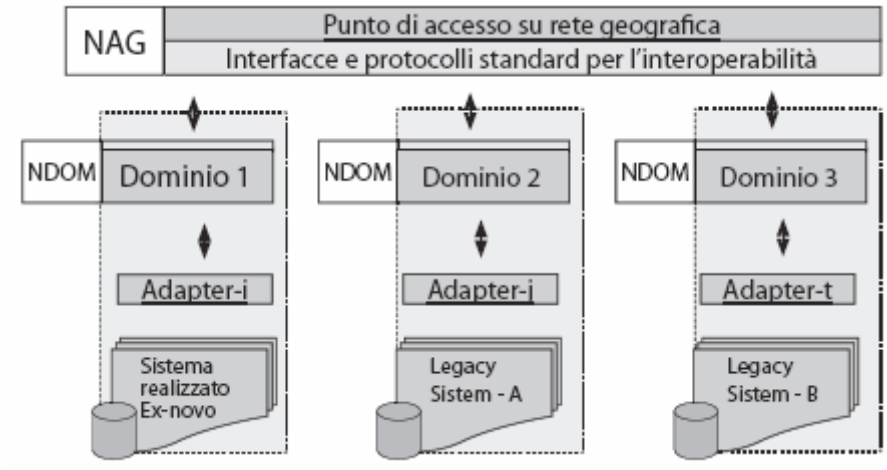
- nelle Sezioni 3 - 6 viene dettagliato il sistema da realizzare,
- nelle Sezioni 7 e 8 sono illustrati il sistema di anagrafe e i servizi applicativi della rete MMG/PLS.

Prerequisito fondamentale per il corretto funzionamento del sistema oggetto del presente capitolato è il raggiungimento del requisito di interoperabilità, basato sulla definizione di un insieme di regole standard e componenti architetturali che vanno a realizzare lo strato di intermediazione tra gli attori del sistema. La Figura 5 (Sezione *Componenti Logici dell'Architettura*) mostra un modello logico di riferimento di elaborazione distribuita, dove ogni singola infrastruttura informatica è vista come un dominio unitario vincolato a meccanismi standard di interfacciamento. Per poter garantire l'interfacciamento, ogni dominio può utilizzare uno specifico componente di adattamento, il cui compito è rendere possibile, secondo modalità standard di interazione e regole standard, la percezione dei sevizi per la Rete dei Medici come qualcosa di integrato.

Il sistema che si chiede di progettare deve rispondere a requisiti di compatibilità con il modello regionale SPICCA, nel quale esistono due tipologie di nodi funzionali:

• **Nodi di aggregazione** (NAG) per la integrazione e gestione di servizi di supporto all'interoperabilità. Tale nodo può avere sia la funzione di rendere omogenei e integrati servizi di una stessa natura offerti da diversi soggetti per offrire uno stesso servizio su più ampia scala, che di integrare mediante interfacce standard diverse tipologie di servizi per offrire un nuovo servizio complesso a valore aggiunto. Ne deriva che il nodo aggregatore può essere visto come composto da due macro componenti: una di supporto base alla cooperazione ed una con funzioni più significativamente legate alla gestione dei particolari servizi di riferimento. La funzione del nodo aggregatore può anche essere semplicemente quella di supporto all'interoperabilità, limitandosi ad esempio alla sola pubblicazione di servizi di competenza di altri domini o di altri nodi aggregatori.

• **Nodi di dominio** (NDOM) per l'accesso ai servizi applicativi di un soggetto, che integrano eventuali sistemi di adattamento, inclusa la presenza di eventuali componenti di adattamento o connettori ai sistemi informativi locali interoperanti. Tali nodi possono offrire servizi in modo autonomo e/o attraverso nodi di aggregazione.



In particolare, per il progetto oggetto del capitolato cui il presente documento è allegato, si richiede la costruzione di un Servizio di aggregazione/intermediazione per la rete dei Medici di Medicina Generale (SAMMG), tenendo conto che le componenti sussidiarie e di supporto alla cooperazione risultano essere già presenti presso il componente architetturale "Nodo Aggregatore" della Regione Campania. Pertanto, relativamente al SAMMG, è necessario realizzare solo le interfacce di integrazione verso gli specifici gateway applicativi per i servizi della Rete dei MMG/PLS.

2 CONTESTO EVOLUTIVO DEL SISTEMA NAZIONALE DI SANITÀ ELETTRONICA

Questo paragrafo contiene alcune indicazioni sul *contesto evolutivo* del Sistema Nazionale di Sanità Elettronica. Esse non sono oggetto di fornitura del presente capitolato, ma vengono riportate per completezza, in modo che il fornitore:

- abbia una visione di come sta evolvendo l'infrastruttura nazionale di Sanità Elettronica
- realizzi un sistema regionale (descritto nella sezione seguente) per la messa in rete dei MMG/PLS che sia coerente con tali caratteristiche, e di conseguenza, facilmente integrabile con il futuro sistema nazionale che prevede l'interoperabilità di tutti gli operatori sanitari su scala nazionale.

Inoltre, nella fase di progettazione esecutiva del sistema regionale occorrerà tenere conto dei documenti pubblicati dal Tavolo di Lavoro Permanente Sanità Elettronica che definiranno l'architettura dell'Infrastruttura di Base della Sanità Elettronica (IBSE) a livello nazionale. IBSE è composta dalle seguenti componenti logiche:

- Infrastruttura SPCC per la comunicazione tra tutti gli operatori sanitari (i MMG/PLS, gli specialisti, i laboratori, le Aziende Ospedaliere, ecc.) basata sugli standard CNIPA[1] per l'interoperabilità, ed in particolare sui principi delle Architetture Orientate ai Servizi (Service Oriented Architetture - SOA).
- IBSE network: un servizio per l'indicizzazione ed il routing delle informazioni relative agli eventi sanitari individuali su scala nazionale tra gli attori autorizzati; tale servizio è chiamato InfoBroker Individuale Sanitario (IBIS);
- Moduli per l'interoperabilità Semantica e Sintattica tra i documenti elettronici basati su standard internazionali riconosciuti (HL7 v.3, ed in particolare Clinical Document Architecture v2 per la messaggistica, DICOM, ecc.);
- un sistema integrato di servizi e processi sanitari on line quali, ad esempio: prescrizione, refertazione, prenotazione, certificazione di malattia, certificazione parto, malattie croniche, ecc.;
- Politiche di sicurezza e privacy: per garantire l'accesso sicuro al sistema, attraverso firma digitale ed autenticazione forte (standard CNS[2]) e nel rispetto degli standard nazionali e dei più diffusi standard internazionali.

Figura 1 - Infrastruttura di Base della Sanità Elettronica

Il Tavolo di lavoro permanente di Sanità Elettronica (TSE), in cui tutte le Regioni e le Province Autonome sono coinvolte, insieme al Ministro dell'Innovazione e delle Tecnologie e al Ministero della Salute, è il luogo dove vengono cooperativamente definiti e/o adottati gli standard, in ambito sanitario.

1 http://www.cnipa.gov.it
2 Vedi: http://www.cnipa.gov.it

In questo contesto IBSE è pensata per avere la minima invasività rispetto alle infrastrutture regionali che potranno integrarla rispetto alle proprie specifiche esigenze, ma che tuttavia devono convergere verso un'architettura nazionale interoperabile.

Il nucleo centrale di IBSE è l'InfoBroker Individuale Sanitario e realizza il Fascicolo Sanitario Elettronico (FSE), come mostrato in Figura 2.

L'FSE permetterà di raccogliere e accedere in modo sicuro e nel rispetto della privacy alle informazioni di dettaglio, indipendentemente da dove queste siano disponibili e da quale luogo siano richieste. I repository dipartimentali e/o regionali interessati sono tutti quelli coinvolti nei processi che consentono di assicurare la continuità dell'assistenza e cura del paziente, ovvero, per citarne alcuni, l'accettazione, l'anagrafe sanitaria, il centro unico di prenotazione, i laboratori di analisi, la radiologia, i reparti, il pronto soccorso, l'anatomia patologica, le cartelle cliniche dei medici di medicina generale, le farmacie, ecc.

Figura 2 - Fascicolo Sanitario Elettronico

Nella Figura 3 viene fornita, a scopo puramente illustrativo, una rappresentazione del sistema, in cui viene esplicitata la funzionalità di indicizzazione su scala nazionale del FSE, che tiene conto:

- delle specifiche CNIPA SPCC
- della struttura federata del Sistema Sanitario Nazionale
- dei principi delle Architetture Orientate ai Servizi (Service Oriented Architetture - SOA)
-

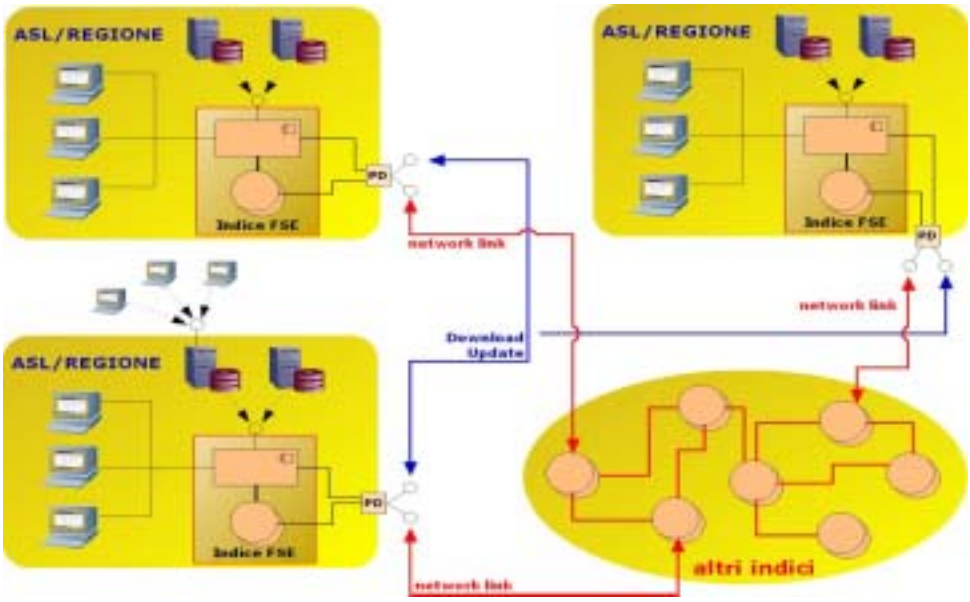
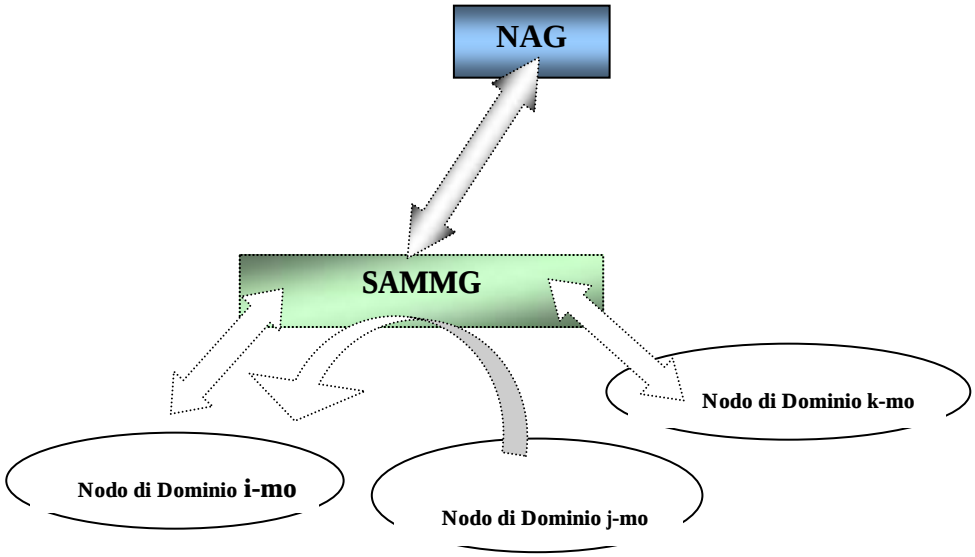


Figura 3 - Un'architettura federata del sistema (a carattere illustrativo)

3 ARCHITETTURA REGIONALE DI RIFERIMENTO DEL SISTEMA DI AGGREGAZIONE PER LA RETE DEI MMG

In questo paragrafo vengono presentate le linee guida di un sistema regionale per la messa in rete dei MMG/PLS. Coerentemente con esse, il fornitore dovrà fornire una soluzione progettuale e realizzativa relativamente a:

- i servizi applicativi che un sistema integrato deve offrire ai Medici di Medicina Generale, rispettando la descrizione delle funzionalità e casi d'uso riportate nelle sezioni seguenti;
- i servizi di base per l'interoperabilità (SAMMG);
- Il Fascicolo Sanitario Elettronico.



Modello di funzionamento del SAMMG e relazione col NAG

Il SAMMG rappresenta un servizio di aggregazione che può inscriversi a sua volta nel NAG della Regione Campania; il SAMMG rappresenta quindi un elemento per ottenere l'integrazione dei servizi della Rete dei MMG/PLS, con speciale riguardo a quelli relativi al fascicolo sanitario elettronico interoperabile. Inoltre, il SAMMG si interfaccia con tutte le componenti del sistema che offrono funzionalità per l'adattamento dei servizi e che costituiscono i vari Nodi di dominio (mostrati nella figura precedente).

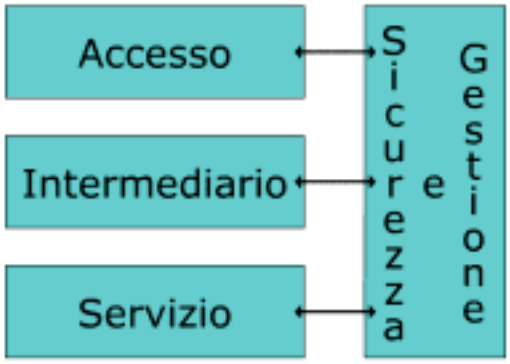
Il sistema per la messa in rete degli MMG/PLS a livello regionale deve:

- essere disegnato e realizzato utilizzando i principi del modello SPICCA ed in particolare potersi rifare ad architetture sia di tipo Event Driven Architecture (EDA) che di tipo Service Oriented Architecture (SOA);
- effettuare l'accesso ai servizi tramite web service secondo le specifiche SPCC. Questo garantisce l'interoperabilità tra sistemi progettati in maniera indipendente (condividendo i protocolli di comunicazione), realizzando così l'obiettivo dell'accoppiamento lasco (loosely coupled) delle architetture SOA. Inoltre, occorre prediligere soluzioni non proprietarie basate su standard aperti.
- utilizzare per la messaggistica lo standard HL7 Versione 3 ed in particolare la Clinical Document Architecture (CDA) versione 2.
- garantire adeguati livelli di sicurezza e privacy, nel rispetto degli standard nazionali e dei più diffusi standard internazionali.
- essere opportunamente dimensionato per assicurare performance e livelli di servizio adeguati a garantire continuità di servizio (affidabilità del funzionamento 24 ore su 24).

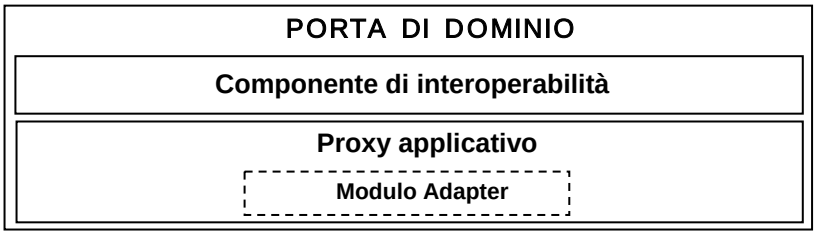
Inoltre, le interfacce utente, dove realizzate, devono essere il più possibile user-friendly ed accessibili agli utenti, indipendentemente dal loro grado di esperienza informatica.

I Nodi di Dominio vengono visti come centri di 'business process', ossia espongono i servizi applicativi che devono accedere all'insieme di risorse ed applicazioni in grado di eseguire l'intero processo di business. In ogni caso, per consentire la piena autonomia ai nodi di dominio, è importante evidenziare

che i servizi offerti da un Nodo di Dominio possono essere acceduti anche direttamente senza utilizzare eventuali adattatori e continuando ad utilizzare i meccanismi locali di controllo degli accessi. Il SAMMG dovrà essere strutturato secondo le componenti:



Per quanto riguarda le componenti architetturali porte di Dominio da realizzare invece dovranno garantire le componenti:



Presso i Nodi di dominio saranno implementate le componenti software di cooperazione applicativa tra i vari attori del sistema . Esse forniscono servizi per le applicazioni che devono interoperare, sia all'interno del dominio stesso che verso altri sistemi esterni, quali ad esempio sistemi informativi ospedalieri e/o applicazioni utilizzabili da personale sanitario preposto alle cure d'emergenza, mettendoli nelle condizioni di poter utilizzare in modalità controllata ed efficiente le informazioni sanitarie dei pazienti.

L'interoperabilità, anche in campo sanitario, si ottiene, quindi, attraverso l'applicazione delle condizioni di seguito riportate:

- applicazione di standard per il formato dei documenti e dei dati trasmessi, secondo anche quanto indicato nelle specifiche CNIPA di "Busta di e-Gov";
- 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.

Una volta definite le funzionalità che si intendono implementare, affinché il modello cooperativo possa realmente essere utilizzato, è necessaria una preliminare definizione del contenuto completo e del formato di codifica dei dati e dei messaggi a cui ogni funzionalità può accedere durante una transazione per l'erogazione del servizio. Risulta evidente che la definizione dei formati deve fare necessariamente uso di standard aperti favorendo da un lato la cooperazione ed evitando, dall'altro, la proliferazione di dati strutturati in modo proprietario che renderebbe arduo, se non impossibile, il compito di integrazione di servizi e dati.

A tal proposito, si adotta la struttura più generale dei messaggi scambiati tra le porte di Dominio, utilizzando le specifiche CNIPA di "Busta di e-Gov"[3]. Esse prevedono lo scambio di messaggi XML

[3] Si rimanda al documento CNIPA, *Sistema pubblico di Cooperazione: Busta e-Gov*, Versione 1.0, 14 ottobre 2005, www,cnipa.gov.it

usando il protocollo SOAP: essi rappresentano infatti gli attuali standard aperti di riferimento per la strutturazione dei dati e dei servizi, e la definizione dei protocolli di interscambio. L'elemento principale di un messaggio è rappresentato dalla struttura XML/SOAP composta da due parti, ovvero intestazione e descrizione:

- l'intestazione (XML/SOAP Header) contiene i dati relativi al messaggio ed in particolare contiene l'identificativo del messaggio, che coincide con l'identificativo di protocollo;
- la descrizione (XML/SOAP Body) riporta i dati riguardanti il contenuto applicativo del servizio; tali dati possono includere l'insieme completo delle informazioni riguardanti la request/response oppure limitarsi alla semplice indicazione del tipo di documento informatico allegato e del relativo formato di codifica.

Dal punto di vista amministrativo, la strutturazione dei dati fatta in questo modo,offre la possibilità di avere una segnatura informatica del messaggio in quanto riporta i dati minimi sufficienti per la registrazione di protocollo. Inoltre, linguaggi come XML , data la loro estendibilità, possono essere usati, in combinazione con altri standard, anche per la descrizione dei servizi o per la realizzazione dei repository di descrizione dei servizi. La struttura XML/SOAP può inoltre includere una struttura MIME allo scopo di allegare al messaggio uno o più documenti applicativi, in base allo standard XML/SOAP with attachments. Ad esempio potrebbe essere allegato un documento su cui è stata apposta la firma di un medico o di uno specialista. La presenza degli allegati è comunque opzionale.

Una firma opzionale può essere inclusa nell'intestazione utilizzando gli standard XML/SOAP Security e XML Signature e potrebbe, ad esempio, essere usata per garantire la fonte di provenienza delle informazioni. Nel caso di documenti informatici firmati aventi rilevanza legale è adottato il formato il PKCS#7 in base alla circolare AIPA CR/24.

Sarà necessario inoltre permettere il collegamento della Rete dei Medici di Medicina Generale all'infrastruttura di rete regionale RUPAR, fornendo il collegamento dei nodi di dominio alla rete regionale.

Le componenti di cooperazione ed integrazione permettono, invece, di tenere allineate le informazioni sanitarie dei cittadini assistiti. In particolare devono essere garantite tutte le funzionalità seguenti:

- gestione degli eventi contenenti i dati clinici degli assistiti, nel rispetto della normativa vigente sulla privacy;
- allineamento delle banche dati dei sistemi interoperanti;
- gestione della Porta di dominio a supporto della piattaforma cooperativa.

Il Sistema sarà caratterizzato anche dai seguenti requisiti non funzionali:

- Sicurezza: rispetto delle norme previste in termini di sicurezza informatica ed utilizzo di robusti strumenti di difesa contro le intrusioni;
- Flessibilità: poter gestire le evoluzioni organizzative, di processo e normative che accompagneranno il sistema nel corso del tempo;
- Portabilità, riusabilità, modularità ed estensibilità: ogni attore coinvolto può, indipendentemente dalla tecnologia, decidere quali componenti utilizzare dell'infrastruttura a seconda delle proprie necessità;
- Usabilità e facilità di gestione;
- Rispetto degli standard e protocolli (Web services, SOAP, WSDL, UDDI, XML, J2EE, WS-transaction, SAML, PKI, …).

3.1 Componenti Logici dell'Architettura

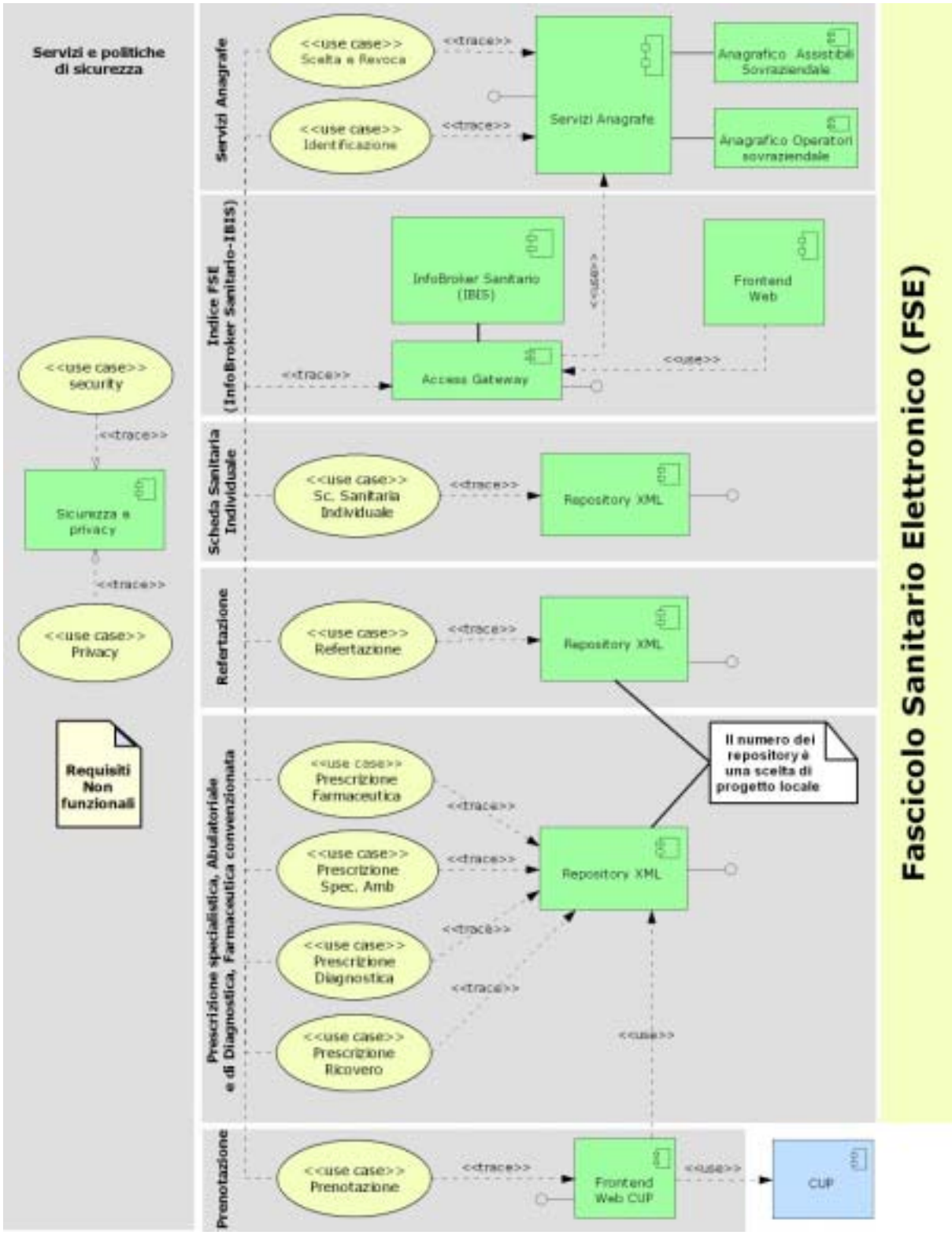


Figura 4 - Architettura di riferimento regionale - Use case e componenti funzionali

La Figura 4 illustra i servizi funzionali che un sistema integrato regionale deve offrire ai Medici di Medicina Generale

- **Servizi di identificazione degli operatori sanitari**
- **Servizi di identificazione degli assistiti**
- **Servizi di scelta e revoca MMG/PLS**

- **Servizi di prescrizione specialistica, ambulatoriale e di diagnostica (strumentale e di laboratorio), farmaceutica convenzionata e di ricovero**
- **Servizi di Refertazione**
- **Interfacciamento con il sistema CUP Integrato Regionale**
- **Fascicolo Sanitario Elettronico**
- **Front end FSE e Scheda Sanitaria Individuale**

I suddetti servizi devono essere supportati da componenti trasversali che garantiscono la sicurezza del sistema.

Per una descrizione dettagliata dei servizi si rimanda al paragrafo *Servizi applicativi della rete MMG/PLS* dell'*Allegato E – Capitolato Tecnico*.

3.1.1 Fascicolo Sanitario Elettronico

L'architettura del Fascicolo Sanitario Elettronico prevede un indice degli eventi (Infobroker Sanitario - IBIS) e una serie di repository relativi ad eventi/documenti[4] sanitari (es. referto di laboratorio, prescrizione, ricovero), ciascuno dei quali è un'entità indipendente. Ciascun repository memorizza e mantiene la responsabilità dei dati archiviati. In presenza di ogni nuovo evento sanitario, il sistema dell'operatore sanitario memorizza l'informazione di dettaglio dell'evento in un repository, che a sua volta effettua una notifica all'indice degli eventi del Fascicolo Sanitario Elettronico.

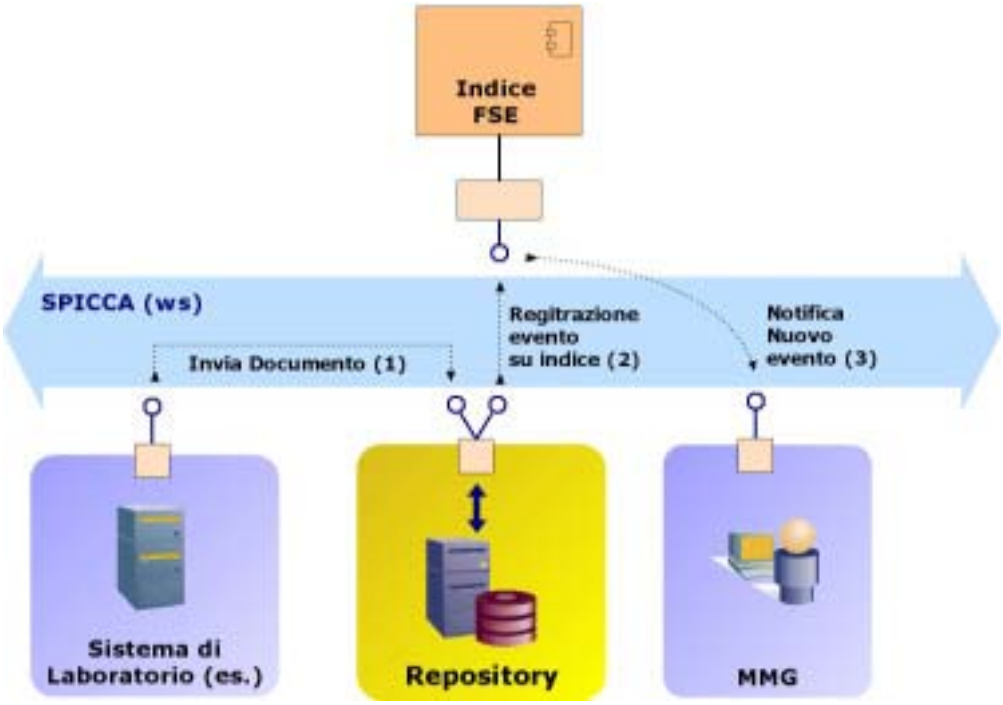


Figura 5 - Indice FSE (Infobroker Sanitario - IBIS)

L'indice registra i metadati del documento e la locazione di quest'ultimo ed effettua una notifica al MMG/PLS dell'assistito (cui l'evento sanitario si riferisce), come illustrato in Figura 5. Il MMG/PLS (e più in generale qualunque operatore sanitario autorizzato), attraverso la notifica dell'evento o attraverso una interrogazione del FSE, potrà recuperare le informazioni di dettaglio dell'evento sanitario che risiederanno presso la struttura sanitaria dove l'evento è stato generato, come illustrato in Figura 6.

[4] Per evento sanitario si intende qualunque episodio assistenziale a carico di un paziente.

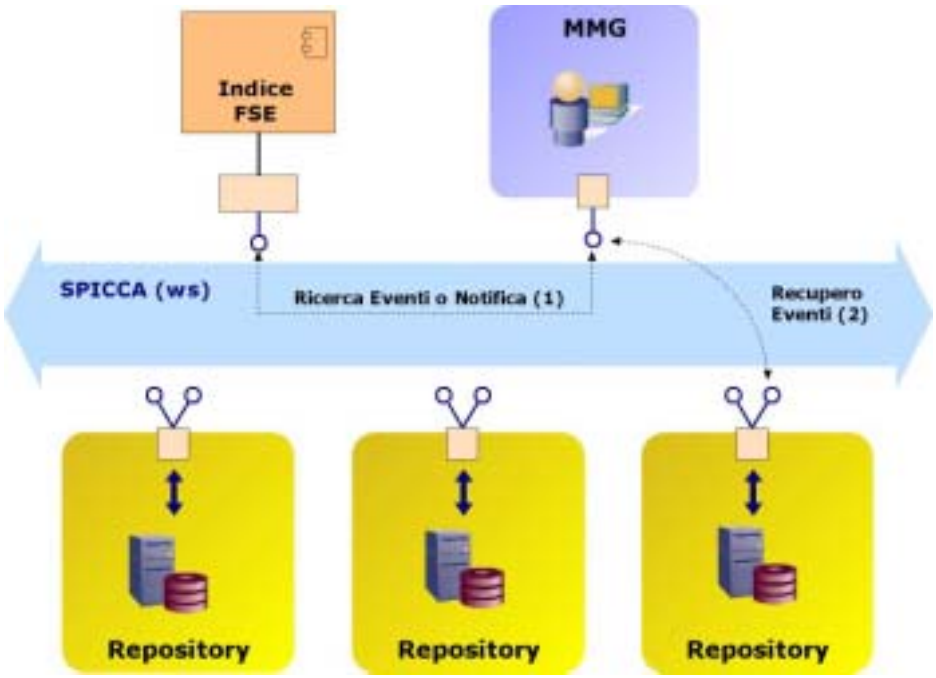


Figura 6 - Ricerca e recupero eventi

Relativamente alla realizzazione del fascicolo, il sistema deve prevedere:

- **un indice degli eventi sanitari (Infobroker Sanitario - IBIS) direttamente associato all'anagrafe sanitaria della popolazione assistita.** L'indice, come già osservato, non contiene i dati clinici, che rimangono nel repository della struttura sanitaria che li ha prodotti, ma contiene i riferimenti agli eventi sanitari (intesi come documenti) dell'assistito. L'indice presenta all'utente autorizzato l'elenco degli eventi e, a richiesta restituisce l'indirizzo del servizio in cui è contenuto il documento richiesto che viene scaricato, in modo trasparente, all'utente dal repository che lo contiene. La presentazione è effettuata tramite un componente (access gateway) che riassembla le informazioni sia attraverso un'interfaccia utente che una programmatica e che supporta il recupero delle informazioni dalle sorgenti originali.
- **sistemi di repository per la memorizzazione degli eventi sanitari degli assistiti.** Questi sistemi devono poter essere distribuiti o accentrati in un unico sistema regionale a seconda delle scelte che in sede operativa verranno effettuate per rispondere alle esigenze e alle possibilità di gestione. I repository contengono documenti XML prodotti, con modalità diverse, da attori del sistema (es. centri di analisi, di diagnosi, ecc.) che si interfacciano con questi e con l'indice degli eventi.
- **interfacce per la comunicazione con le diverse strutture degli operatori sanitari (MMG/PLS, ASL, Azienda Ospedaliera, Policlinici Universitari)** presenti sul territorio Regionale, con la relativa stesura dei protocolli per l'interscambio dei dati, basati su standard HL7 v3.
- **funzioni di sicurezza** in modo che l'accesso dell'assistito al sistema dei fascicoli sia consentito inizialmente attraverso l'utilizzo di userID e password, rilasciati in modalità controllata all'assistito stesso. Il sistema dovrà essere predisposto affinché l'accesso al sistema da parte dell'assistito avvenga tramite la Carta Nazionale dei Servizi o la Carta di Identità Elettronica. L'accesso degli operatori avverrà invece fin da subito tramite carta operatore (CNS).

4 FUNZIONALITÀ DEL SISTEMA

Data l'architettura di riferimento, le funzionalità che il sistema oggetto del presente capitolato 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.

4.1 Funzionalità per l'integrazione e l'interoperabilità

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, ricerca/individuazione e presentazione dei servizi.

4.2 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.

In accordo con quanto discusso nella Sezione *Requisiti relativi alla sicurezza* dell'*Allegato E - Capitolato Tecnico*, tutti i componenti dell'architettura in grado di offrire funzionalità di sicurezza, devono includere:

- Servizi di controllo degli accessi,
- Servizi di certificazione (in particolare, tali servizi sono di competenza del NAG regionale),
- 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).

4.3 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.

4.4 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 SAMMG. In particolare, data la particolare importanza di tali servizi, dovrà essere previsto un servizio di logging e tracciamento sia di livello locale, per ogni sottosistema coinvolto, che di livello gerarchico superiore per la gestione centralizzata.

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.

4.5 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 SAMMG, e con essi le metriche di valutazione relative all'accordo di servizio che regolamenta il colloquio tra i sottosistemi cooperanti.

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.

Al fine di identificare le funzioni proprie del SAMMG, si fa presente che per i servizi elencati nella sezione 3.1 il componente SAMMG ha il compito di monitorare il livello di servizio rispetto al livello dichiarato; per i servizi offerti dal SAMMG, devono essere monitorati gli SLA definiti.

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

5 COMPONENTI DEL SISTEMA PER LA REALIZZAZIONE DEI SERVIZI DI BASE PER IL SISTEMA DI AGGREGAZIONE PER LA RETE DEI MEDICI

Il SAMMG che si intende realizzare è un aggregatore di servizi ossia un elemento capace di offrire i servizi del livello NDOM in modo integrato. In particolare, nel SAMMG non sono presenti quei servizi sussidiari alla cooperazione applicativa propri del NAG regionale.

Le caratteristiche proprie di un SAMMG che si propone come aggregatore di servizi sono:

- assicurare la fruibilità dei servizi esposti;
- 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.

Il SAMMG deve essere tale da poter interagire con il Nodo Aggregatore in fase di realizzazione presso la Regione Campania (NAG).

Per poter interoperare, il SAMMG deve essere realizzato seguendo le specifiche definite dal Nodo Aggregatore della Regione Campania (NAG) che 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 servizi da aggregare.

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 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 le seguenti componenti funzionali che si devono realizzare ed integrare:

- componenti per l'integrazione e l'interoperabilità,
- componenti base per la realizzazione di servizi aggregati,
- componenti per la gestione della sicurezza,
- componenti per la gestione dell'accesso multicanale,
- componenti per la tracciabilità,
- componenti per il monitoraggio della qualità dei servizi.

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

Il sistema dovrà essere opportunamente dimensionato affinché possa, a regime, gestire oltre 5.000 utenti registrati (utenti di Pubbliche Amministrazioni, Enti Privati e cittadini) e oltre 100 servizi da esporre.

E' richiesto come vincolo imprescindibile del progetto che:

- ogni componente realizzato possa 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;
- sia previsto un accesso anche in termini di web services (per i componenti per i quali ciò abbia senso);
- ogni componente realizzato sia indipendente dalla soluzione tecnologica adottata per gli altri componenti in modo da favorire un eventuale sua sostituzione o modifica;
- l'architettura sia 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.

5.1 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
- SOAP
- UDDI
- WSDL

5.1.1 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 l'indirizzo dei servizi.

Grazie a questo modello scalabile è possibile preservare e rispettare le autonomie dei sistemi preesistenti. In altri termini, l'architettura può essere vista, secondo scenari alternativi, come:

- servizio unico aggregato che può inscriversi nel registro NAG regionale;
- i singoli servizi applicativi possono iscriversi nel registro di SAMMG;
- i singoli servizi applicativi possono iscriversi nel registro del NAG regionale.

Sarà cura del fornitore presentare una soluzione progettuale che risponda ad una o più delle alternative proposte.

5.1.2 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.

5.1.3 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 si devono 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.

5.1.4 Specifiche di integrazione ed erogazione dei contenuti Web

L'integrazione di un server Web esistente può avvenire:

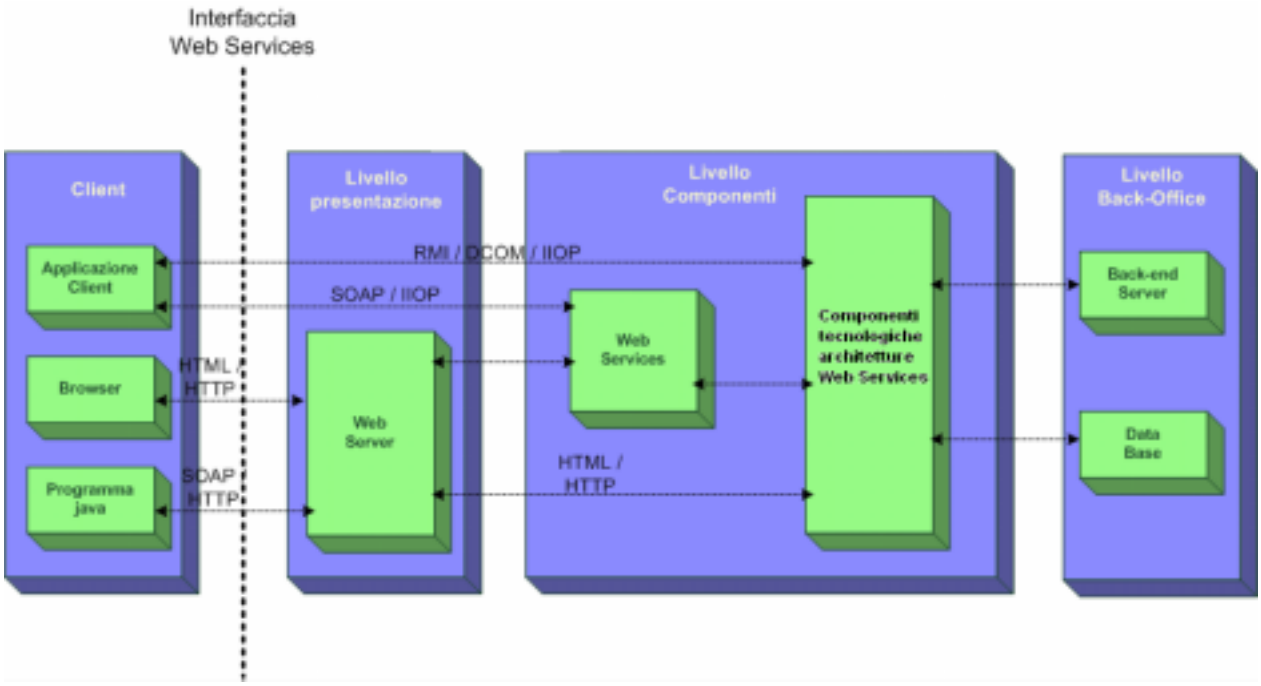
- tramite collegamento ipertestuale: in tal caso il sistema deve unicamente esporre un link del sito web da integrare, rimandando a questi totalmente la gestione dei contenuti
- unificando i contenuti sul sistema: in tal caso è il sistema che espone in maniera diretta i contenuti presenti su altri siti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

5.1.5 Specifiche di integrazione ed erogazione dei Servizi

L'erogazione dei servizi web va intesa nell'ottica dei Web Services (WS) e quindi il SAMMG 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)



5.1.6 Componenti base del SAMMG per la realizzazione di servizi aggregati

Il SAMMG 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 SAMMG 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 in precedenza; esso deve essere in grado di interagire con i sistemi terminali di accesso (sia utenti esterni che altri servizi) e deve 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 SAMMG dunque garantisce ed ottimizza l'accesso ai diversi servizi. A tal fine, il SAMMG garantisce l'accesso ai servizi che direttamente gestisce, permettendo attraverso le proprie caratteristiche di intermediazione, l'integrazione degli stessi. Lo stesso SAMMG deve poter garantire a servizi non gestiti direttamente (punti di accesso esterni) di potersi integrare con i servizi del dominio gestiti dallo stesso SAMMG. Tutto ciò deve avvenire sempre con 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 sia servizi già esistenti per i medici di medicina generale che servizi nuovi da implementare.

Per la realizzazione delle funzionalità di interoperabilità, il SAMMG 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 SAMMG,

5.1.7 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.

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/semantico analizzando l'interfaccia del servizio ed il corretto funzionamento testando a run time l'applicazione.

5.1.8 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.

5.1.9 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 (del servizio) 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 SAMMG, 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.

5.2 Componenti per la gestione della sicurezza

Il sistema per l'aggregazione, 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) implementare meccanismi di autenticazione ed autorizzazione "forti" e "deboli";
2) 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 servizi.
3) implementare la sicurezza per i Web Services, per i server web e per tutti i componenti del sistema.

In particolare, il primo 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, ad esempio Carta Nazionale dei Servizi, Carta di Identità Elettronica, o compatibili;

Tra i meccanismi forti si prediligono, inoltre, soluzioni che prevedono l'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 dai servizi o centralmente sul nodo SAMMG;
- 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 devono includere:

- Controllo degli accessi,
- Monitoraggio ed Auditing.

I dettagli dei componenti sono illustrati di seguito al fine di esemplificare alcune condizioni operative del sistema.

5.2.1 Modello di riferimento per il controllo degli accessi

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.

Le componenti principali per la definizione degli utenti e dei loro privilegi, e per la gestione delle loro attività sono:

- *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.

Parte integrante è anche un 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 per il Risk Assesment.

5.2.2 Specifiche per la sicurezza

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.

Vi sono quattro possibili scenari di Autorizzazione 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 SAMMG, e richiamabile tramite interfacce standard da tutti i domini. Le interfacce devono essere tali da poter garantire un'unica autenticazione sul SAMMG, ed attraverso la gestione di un contesto di sicurezza associato ad una sessione di lavoro, si permetta di operare in modo trasparente attraversando domini o servizi diversi senza dover reiterare le operazioni di autenticazione-autorizzazione.

Resta comunque valida, la possibilità di poter gestire il controllo degli accessi in modo autonomo dai singoli servizi 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.

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

Specifiche per l'accesso in sicurezza dei Web Services

I servizi erogati dai Web Services devono anch'essi presentare un livello di sicurezza adeguato, risultato dei processi di Risk Assessment e Risk Management, che sarà richiesto nello sviluppo del progetto secondo quanto indicato nella Sezione *Piano per la Sicurezza* dell'*Allegato E - Capitolato Tecnico.* 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 middleware 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.

5.2.3 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 la Certificazione di identità e privilegi;
- Componenti per il Monitoraggio e l' Auditing.

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 o 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 del Fornitore 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.

Componenti per la Certificazione di identità e privilegi

Gli utenti che possono rivestire dei ruoli specifici devono essere registrati presso una Certification Authority (CA del NAG regionale) ad uso interno e presso una Attribute Authority (AA del NAG regionale) 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 SAMMG;
- 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 (emesso dal sistema di CA del NAG regionale) 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.

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.

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.

5.3 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.

5.4 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 SAMMG 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.

5.4.1 I servizi da tracciare

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)

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.

5.5 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

5.5.1 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 SAMMG che dagli NDOM.

La formalizzazione dei livelli di servizio attesi (Service Level Agreement) è definita avanti, e sono anche indicati, quali sono, nello specifico, i parametri qualitativi e quantitativi che devono essere soddisfatti dai servizi offerti dal SAMMG.

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 SAMMG che di NDOM, a tal proposito occorre precisare che gli SLA definiti nella Sezione *Valutazione dei livelli di servizio* dell'*Allegato E - Capitolato Tecnico* sono relativi ai servizi base e di aggregazione del SAMMG, 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 SAMMG.

Alla luce di quanto detto, deve essere possibile identificare e monitorare eventuali colli di bottiglia nel processo, che parte dal SAMMG 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 dei nodi di dominio "attivi" nel sistema. Tale funzionalità deve poter essere attivata sempre dal sistema di gestione del monitoraggio. 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.

6 COMPONENTI PER L'IMPLEMENTAZIONE DEI NODI DI DOMINIO

A livello architetturale la componente da realizzare per il dominio dei servizi applicativi (DSA) è rappresentata dalla Porta di dominio[5]: essa rappresenta l'elemento logico che ha la funzione di Proxy applicativo per l'accesso alle risorse applicative del dominio. I ruoli tipicamente assunti dalla Porta di dominio sono:

- Porta Applicativa
- Porta Delegata;

Nel primo caso, nell'ambito di un episodio di collaborazione applicativa, essa è predisposta a ricevere un messaggio di richiesta e ad inviare al mittente uno di risposta; nel secondo caso è la Porta di dominio a generare un messaggio di richiesta verso un'altra Porta di dominio nell'ambito di un episodio di collaborazione applicativa.

Una porta di dominio è dunque in grado di ricevere e trasmettere messaggi da e verso (porte di dominio di altri) DSA. Essa può rappresentare uno o più DSA contemporaneamente, con i quali dialoga attraverso protocolli standard implementati dai Listener o protocolli ad hoc implementati da specifici Connector. L'elemento caratterizzante della Porta di dominio è la modularità, grazie alla quale essa si presenta come un componente software estremamente flessibile e scalabile, aperto ad evoluzioni tecnologiche e funzionali. Con la figura seguente si vuole porre in risalto l'aspetto modulare illustrando un esempio di architettura (generale) della porta di dominio.

Con il termine Adapter si vogliono indicare i moduli software che consentono lo scambio di informazioni secondo le regole dettate da specifici protocolli: essi forniscono un insieme di API utili per adattare un messaggio alle specifiche del protocollo di comunicazione adottato e del dominio nell'ambito del quale si realizza lo scambio di messaggi.

[5] Si veda il documento pubblicato dal CNIPA *Sistema pubblico di cooperazione: PORTA DI DOMINIO Versione 1.0,* www.cnipa.gov.it

Il PDD Engine rappresenta il core dell'intero componente: gestisce la comunicazione con tutti gli altri moduli e sa come e quando intraprendere tale comunicazione a seconda del servizio che sta gestendo. Tutte le attività necessarie per realizzare il delivery di un qualunque servizio (Porta Applicativa) o per effettuare l'invocazione di un servizio (Porta Delegata) sono indicate all'interno di tre distinte sequenze di task; le tre sequenze rappresentano le operazioni espletate, rispettivamente, dal gestore della request (Request Handler), che interviene a monte della logica di business del servizio, dal servizio e dal gestore della response (Handler Response), che interviene a valle della logica di business. Ad esempio, se il servizio erogato prevede una signature del messaggio di richiesta, il gestore della request incarica il Message Manager di verificare l'esistenza all'interno del messaggio dei dati necessari e, in caso affermativo, affida al modulo WS Security Manager l'incarico di acquisire tali dati per poi procedere alle necessarie operazioni di verifica. Se tutte le operazioni preliminari espletate dal gestore della request avranno esito positivo (es: validazione, autenticazione e autorizzazione del richiedente, verifica firma, decifratura dati) si procederà ad invocare il servizio, altrimenti verrà prodotto un messaggio di Fault.

Le informazioni necessarie al PDD Engine per poter svolgere la propria attività sono contenute nel *Services Store*, ovvero nel database della Porta di dominio. Tali informazioni sono rappresentate dalle tre sequenze di task di cui al precedente punto, oltre che dai dati necessari per effettuare l'autenticazione ed autorizzazione degli utenti che richiedono i servizi, siano essi appartenenti al DSA della Porta di Dominio o un DSA servito dalla Porta di dominio.

Il DB Manager è il modulo che gestisce il database.

Il database contiene anche i dati prodotti a seguito del *tracing* dei messaggi di request e response di ciascun servizio. Dunque, oltre che essere un Services Store, il database è anche un *DSA Store*, uno *Users Store* ed un *Request&Response Store*.

Il Security Manager è il modulo che gestisce le logiche di autenticazione ed autorizzazione. Tale modulo, interrogato dall'engine per verificare se il servizio richiesto dall'utente rientra nel profilo dell'utente stesso, accede allo *Users Store* attraverso il modulo DB Manager; è la configurazione dello specifico servizio a determinare il livello di autenticazione (autenticazione debole: username/password o autenticazione forte: certificato). Qualunque sia il livello di autenticazione previsto dallo specifico servizio, i dati necessari (username/password, certificato) sono contenuti all'interno del messaggio SOAP secondo le specifiche dello standard *WS Security* o all'interno della *query string* (in chiaro o cifrata) accettata dall' *HTTPListener*. La Porta gestisce l'autenticazione mediante *UsernameToken, BinarySecurityToken, Signature* del messaggio, nel caso di messaggio SOAP, e la coppia username/password nel caso di invocazione dell'HTTPListener. I certificati gestiti sono di tipo RSA, sia nel presente modulo che nel modulo *WS Security Manager*; *3DES* è l'algoritmo utilizzato per realizzare l'*encryption*, sia nel presente modulo che nel modulo *WS Security Manager*.

Il WS Security Manager gestisce i dati contenuti nel nodo veicolante le informazioni di sicurezza associate al messaggio SOAP secondo le specifiche e lo schema XML: sia in fase di lettura, nel caso di messaggio ricevuto, sia in fase di scrittura, nel caso di messaggio da inviare, mediante tale modulo l'Engine è in grado validare la struttura del nodo ed entrare nel merito dei dati in esso contenuti, autenticando il mittente, verificando un'eventuale *signature* applicata al messaggio da parte del mittente o applicare a sua volta una *signature* al messaggio da inviare, decifrare eventuali dati *cryptati* ricevuti o cifrare i dati da inviare.

Il Data Manager è il modulo che si occupa della verifica e della trasformazione delle strutture dati scambiate nei messaggi di richiesta e risposta prodotti dai servizi. Tale modulo è interrogato dall'Engine, ad esempio, per "validare" le strutture XML che devono corrispondere a degli schema ben precisi o per trasformare una struttura dati in un'altra che dovrà essere utilizzata nel corso della elaborazione dei messaggi.

Il Message Manager è il modulo che gestisce il messaggio della request e della response. Tale modulo è in grado di gestire messaggi SOAP, fornendo un insieme di API mediante le quali è possibile:

- validare l'intero messaggio SOAP;
- estrarre/scrivere i singoli elementi del messaggio SOAP (envelope, header, body, attachment).

La caratteristica di modularità conferita si traduce nella scelta di non attribuire a questo modulo il compito di entrare nel merito dei contenuti del messaggio, assegnando ad altri moduli tale compito, ciascuno per la porzione di informazione di propria competenza. Tale modulo è destinato a fornire anche API per gestire messaggi diversi dal messaggio SOAP, come ad esempio messaggi JMS.

L' EGOV Manager è il modulo mediante il quale l'Engine è in grado di verificare la coerenza dei dati contenuti nel messaggio ricevuto o di scrivere i dati correttamente nel messaggio da inviare, nel

rispetto dello schema XML, dal punto di vista formale, e delle specifiche del particolare servizio, dal punto di vista logico. Nel caso di incoerenza formale o logica viene prodotto un opportuno messaggio di *Fault*.

Il Listeners & Connectors: i *Listeners* sono moduli software, che implementano protocolli di comunicazione standard (HTTP, SOAP, JMS, etc.) o scritti ad hoc, attraverso i quali la Porta di dominio accetta le richieste provenienti dai DSA. Un esempio è rappresentato dal listener HTTP, che accetta richieste contenenti parametri obbligatori, necessari per l'autenticazione dell'utente e l'individuazione del servizio richiesto dall'utente medesimo, e parametri necessari al servizio richiesto per poter essere eseguito. I *Connectors* sono moduli software attraverso i quali intraprendere una comunicazione con un determinato DSA: essi possono implementare protocolli di comunicazione standard (HTTP, SOAP, JMS, etc.) o protocolli pensati ad hoc per i DSA che non sono in grado di implementare alcun standard. Un esempio di connector ad hoc è un modulo software che esegue l'invocazione di una Stored Procedure o che produce e memorizza un file su file system.

Il Logging & Tracing è il modulo che si preoccupa di registrare tutte le attività svolte dalla Porta di dominio ogni qual volta giunge una richiesta, sia essa proveniente dall'esterno verso un DSA o viceversa, nonché i messaggi gestiti nel corso della elaborazione della richiesta medesima. L'attività di Logging consiste nel registrare su un supporto di memorizzazione (file system) l'attività di ogni singolo task eseguito nella catena di operazioni previste dal servizio invocato. L'attività di Tracing consiste nel registrare su un supporto di memorizzazione (database) i messaggi gestiti da ciascun servizio invocato: per ciascuna richiesta proveniente dall'esterno o da un DSA servito dalla Porta, viene memorizzato l'intero messaggio pervenuto con la *request*, il messaggio ottenuto dal precedente a seguito di elaborazioni preliminari (ad esempio decifratura dei dati), il messaggio prodotto dal servizio e, infine, il messaggio restituito con la *response* (dopo aver effettuato, ad esempio, la cifratura dei dati forniti in output dal servizio).

Lo Scheduler è il modulo che si occupa della schedulazione di alcune attività, quali lo smistamento degli eventi, la cancellazione ed eventualmente il backup dei file di logging e dei record di tracing dei messaggi, il polling del database, l'aggiornamento delle configurazioni dei servizi caricati in memoria, etc.

L' Event Manager è il modulo che si occupa della gestione dei messaggi che incapsulano dati rappresentativi di eventi a cui sono interessati uno o più DSA. Tale modulo si preoccupa di acquisire la notifica dei messaggi suddetti ed effettuarne lo smistamento ai DSA; viene previsto un meccanismo di storage dei messaggi che consente di realizzarne la persistenza qualora uno o più DSA non siano pronti a riceverli nel momento in cui essi pervengono all'Event Manager. Quanto detto fa sì che la componente possa essere utilizzata non solo come Porta di Domino ma anche come gestore degli eventi, svolgendo la funzione di broker tra pubblicatori e sottoscrittori nel tipico modello di comunicazione Publish&Subscribe.

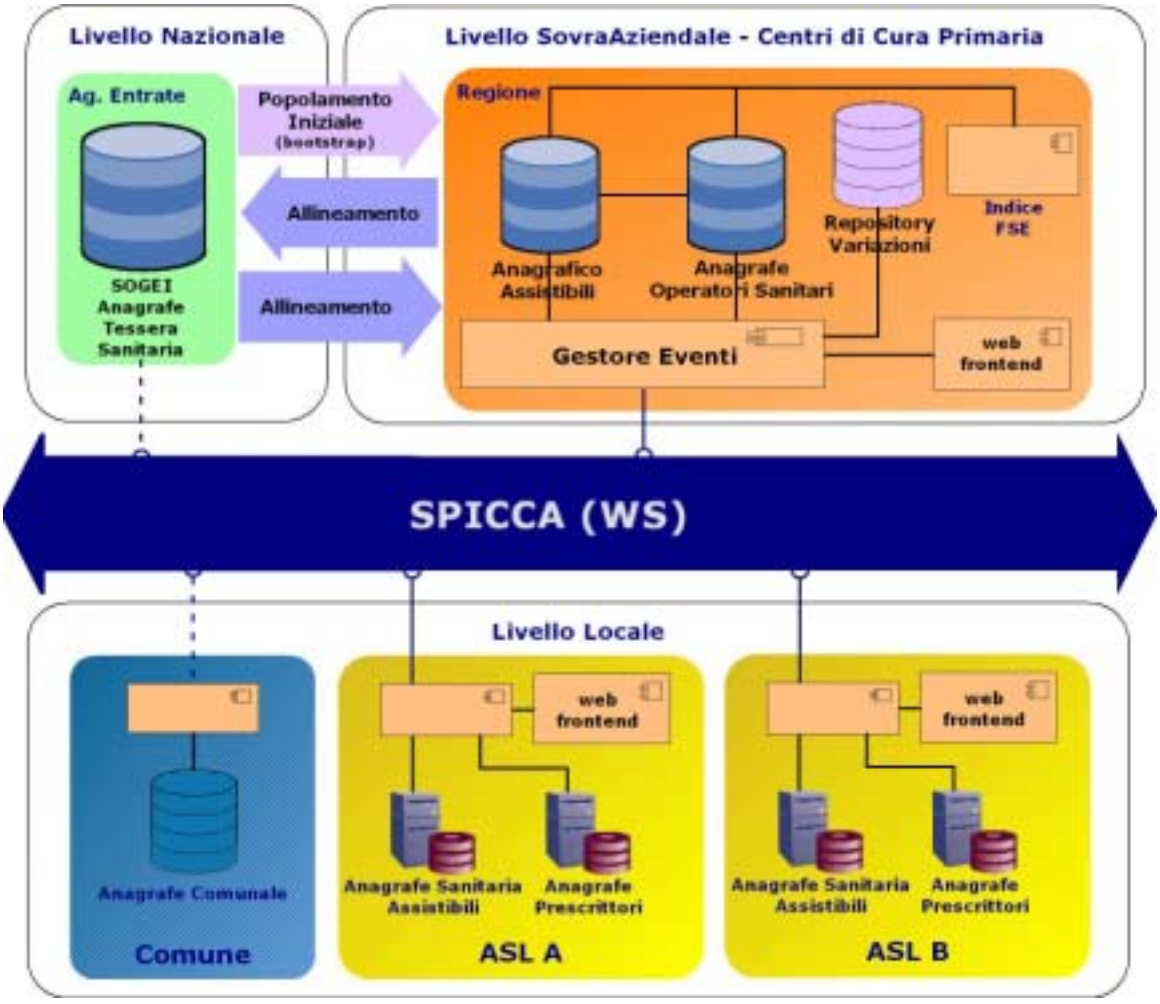
7 SISTEMA DI ANAGRAFE

In quanto segue viene modellato il sistema relativo all'anagrafe, che costituisce un requisito fondamentale per il corretto funzionamento del sistema di cooperazione tra i medici di medicina generale ed i pediatri di libera scelta, il quale offre e realizza i servizi modellati nella Sezione 8. I modelli delle due Sezioni presentano un diverso livello di astrazione: nel primo caso si modella il sistema di anagrafe, nel secondo i servizi offerti ai medici. Il modello di Use Case presentato qui va inteso come un insieme di requisiti minimi e non esaurisce lo scenario d'uso del sistema. Il Fornitore dovrà infatti provvedere all'approfondimento e al completamento di tali requisiti come parte del lavoro di progettazione. Delle specifiche va fornito il modello UML 2.0[6] in formato XMI (OMG Xml Metadata Interchange) e nell'eventuale formato proprietario dello strumento di modellazione concordato all'inizio del progetto. La specifica dovrà comprendere inoltre un documento testuale in formato .rtf e .pdf.

Nella Sezione 7.1 viene introdotta la lista completa degli attori (ruoli) coinvolti negli Use Case che modellano i sistemi di anagrafe e che sono presentati in maniera dettagliata nelle Sezioni 7.2 e 7.3. In fase di progettazione esecutiva tale modello dovrà essere, ovviamente, contestualizzato e dettagliato.

Si noti che tali Use Case rappresentano separatamente i due livelli *sovraziendale e locale*, per cui, ad ogni livello, alcuni attori rappresentano il sistema descritto nell'altro livello. Ad esempio l'Anagrafe Sanitaria Assistibili ASL è modellato a livello *sovraziendale* come attore dell'Anagrafico Regionale Assistibili (Sezione 7.2) e come sistema Anagrafe Sanitaria Assistibili ASL a livello locale nella Sezione 7.3. Si noti che ogni qual volta che si parla di Anagrafe regionale o di livello regionale ci si riferisce al livello "sovraziendale", fermo restando che in un futuro il sistema di Anagrafe sarà esteso all'intera Regione Campania.

Il quadro di insieme è rappresentato nella figura seguente.



6 Vedi: http://www.uml.org.

Figura 7 - Diagramma del sistema delle anagrafi

Nel diagramma in Figura 7 sono rappresentati anche il livello Nazionale (Anagrafe Tessera Sanitaria MEF) e le anagrafi Comunali.

7.1 Attori

Gli attori coinvolti negli Use Case sono i seguenti:

1. MMG/PLS
2. Operatore ASL
3. (Sistema di) Anagrafico Regionale Assistibili
4. (Sistema di) Anagrafe Regionale Operatori
5. (Sistema di) Anagrafe Sanitaria Assistibili ASL
6. (Sistema di) Anagrafe Sanitaria Operatori ASL
7. (Sistema di) Registro Variazioni
8. (Sistema di) Anagrafe Comunale (indicata in blu in quanto già esistente)

Si noti che il Registro Variazioni si limita a realizzare uno storico delle variazioni effettuate. In altre parole, non è altro che un repository, che permette di ricostruire la storia amministrativa di un assistito o di un operatore. Il progetto dovrà ovviamente realizzare le interfacce di interrogazione via web.

Si ricorda che per *assistiti* si intende coloro che hanno assegnato un MMG/PLS, per *assistibili* coloro che hanno diritto all'assistenza (ma non hanno assegnato nessun MMG/PLS).

7.2 Anagrafe Regionale (Livello sovraziendale)

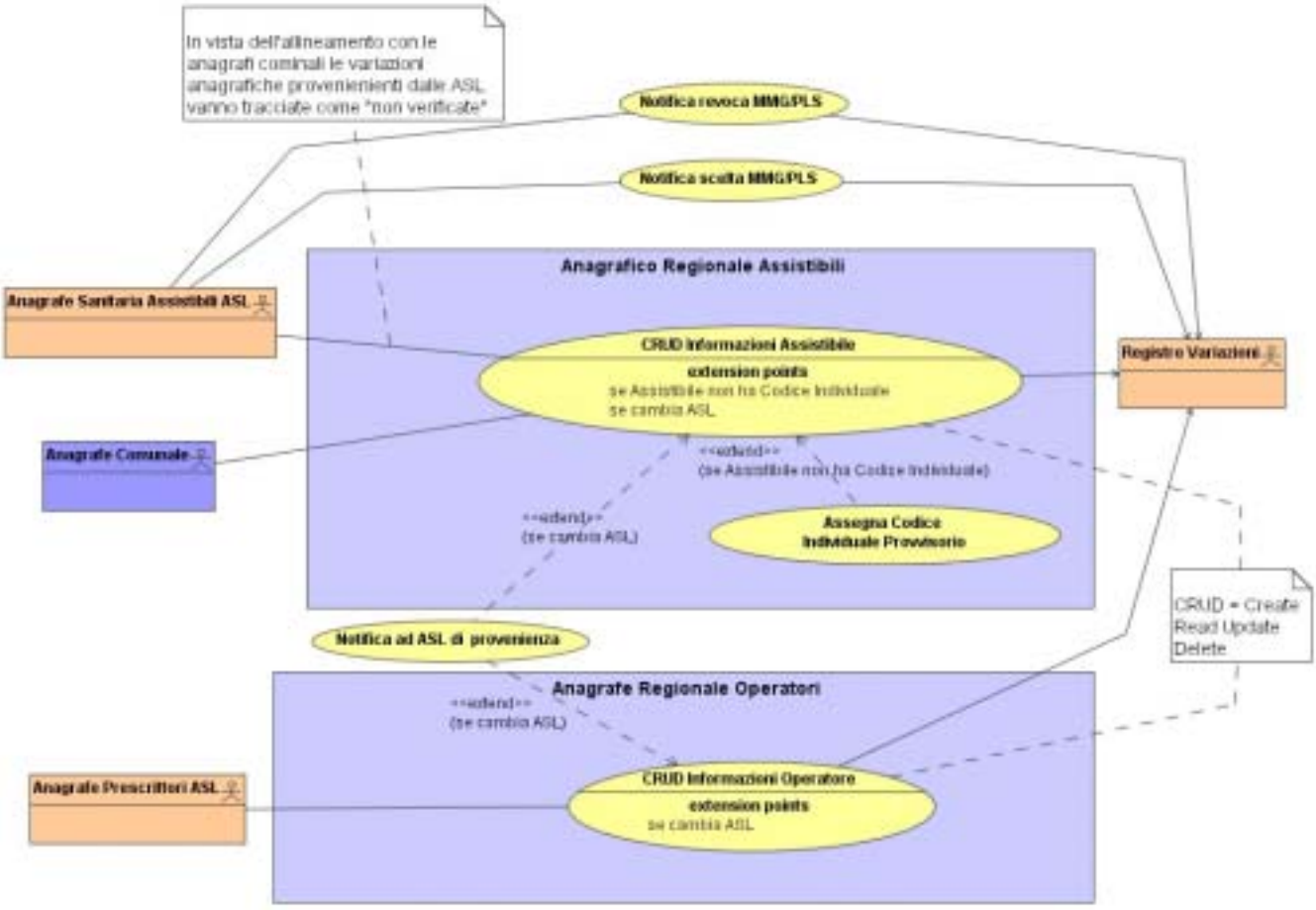


Figura 8 - Sistema di Anagrafe Regionale – Livello sovraziendale

Gli Use Case Package della Figura 8 modellano i servizi che il sistema di anagrafe regionale (operatori e assistibili) fornisce al sistema di anagrafe delle ASL (prescrittori e assistibili) del comune e al registro variazioni. Si noti che:

- l'Anagrafico Regionale Assistibili non va considerato come un'anagrafe centralizzata ma come un indice anagrafico che referenzia l'assistibile e le sue variazioni amministrative (tramite un Registro Variazioni).
- l'Anagrafe Regionale Operatori sarà realizzata replicando l'Anagrafe Prescrittori, attualmente realizzata e gestita dal Ministero dell'Economia e delle Finanze (per effetto dell'intervento previsto dall'Art. 50 D.L. n. 269 del 2003, convertito con modificazioni dalla L. 326/2003), integrandola con i dati relativi agli altri utenti del sistema.

Integrando il sistema di anagrafe regionale con le anagrafi comunali il flusso principale subisce delle variazioni ma le funzioni realizzate negli applicativi rimangono le stesse. Si noti, infine, che gli Use Case esterni ai due Package sono realizzati dal Gestore Eventi presentato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico*. Si ricorda che il Gestore Eventi si occupa di notificare le variazioni alle ASL di competenza.

Relazioni
Association [Anagrafe Sanitaria Assistibili ASL – CRUD Informazioni Assistibile]
Association [CRUD Informazioni Assistibile – Registro Variazioni]

Association [Anagrafe Comunale – CRUD Informazioni Assistibile]
Association [Anagrafe Prescrittori ASL - CRUD Informazioni Operatore]
Association [CRUD Informazioni Operatore - Registro Variazioni]
Association [Anagrafe Sanitaria Assistibili ASL – Notifica Scelta MMG/PLS]
Association [Anagrafe Sanitaria Assistibili ASL – Notifica Revoca MMG/PLS]
Association [Notifica Revoca MMG/PLS - Registro Variazioni]
Association [Notifica Scelta MMG/PLS - Registro Variazioni]
Extend [Notifica ad ASL di provenienza - CRUD Informazioni Assistibile]
Extend [Notifica ad ASL di provenienza - CRUD Informazioni Operatore]
Extend [Assegna Codice Individuale Provvisorio - CRUD Informazioni Assistibile]

7.2.1 Use Case CRUD Informazioni Assistibile

Descrizione

Il servizio permette di creare, modificare, leggere o cancellare le informazioni anagrafiche di un assistibile, contenute nell'Anagrafe assistibili a livello di ASL. Negli ultimi tre casi, è necessario inizialmente ricercare l'assistibile all'interno del sistema, utilizzando, ad esempio, alcuni dei seguenti campi:

- Codice fiscale o Codice Individuale Assistito (provvisorio, fornito quando l'assistito non è ancora in possesso del codice fiscale)
- Nome
- Cognome
- Data di nascita
- Comune di nascita
- Indirizzo di residenza
- Azienda di assistenza
- Azienda di appartenenza
- Codice CNS[7]

Eventuali variazioni anagrafiche devono essere notificate al Registro Variazioni. Lo Use Case *CRUD Informazioni Assistibile* raggruppa gli Use Case elementari che modellano *tutte* le operazioni che possono essere eseguite su un'unità informativa, ovvero, la sua creazione, lettura, aggiornamento e cancellazione. L'acronimo CRUD sta infatti per "Create, Read, Update, Delete".

Extension Points

Tale Use case è esteso dagli Use Case "Assegna Codice Individuale Provvisorio" e "Notifica ad ASL di Provenienza" quando sono rispettate, rispettivamente, le condizioni seguenti:

- l'assistibile non ha Codice Individuale
- l'assistibile cambia ASL (Ricade in tale condizione il caso in cui l'assistibile decede o va in pensione).

Precondizioni

L'attore che accede al sistema deve essere autenticato. Inoltre, nel caso di accesso in lettura, aggiornamento o cancellazione, il cittadino deve essere un assistibile (deve esistere nell'anagrafe il record ad esso relativo).

[7] Il sistema deve essere predisposto per l'utilizzo della CNS.

Postcondizioni

L'attore effettua l'operazione CRUD.

Attori

1. (Sistema di) Anagrafico Regionale Assistibili
2. (Sistema di) Registro Variazioni
3. (Sistema di) Anagrafe Comunale

Note implementative

- Qualora l'assistibile non sia identificato in maniera univoca, verranno mostrate al richiedente le ricorrenze trovate, con l'indicazione dei dati anagrafici sopra elencati per la ricerca, tra le quali verrà selezionata quella di interesse.

7.2.2 Use Case CRUD Assegna Codice Individuale Provvisorio

Descrizione

Scopo di questo servizio è l'assegnazione di un Codice individuale provvisorio ad un nuovo assistibile che ne è sprovvisto, al fine di inserire i suoi dati anagrafici nel sistema. Tale Use Case estende lo Use Case CRUD Informazioni Assistibile quando la condizione dell'extension point "l'assistibile non ha Codice Individuale" è verificata.

Precondizioni

L'attore è autenticato nel sistema e il cittadino è sprovvisto di codice fiscale (e anche di codice individuale provvisorio).

Postcondizioni

Nell'anagrafe regionale viene creato un nuovo record relativo all'assistibile, cui viene associato il nuovo codice individuale provvisorio.

Attori

Tutti e soli quelli dello Use Case CRUD Informazioni Assistibile.

7.2.3 Use Case CRUD Informazioni Operatore

Descrizione

Il servizio permette di creare, modificare, leggere o cancellare le informazioni anagrafiche di un operatore sanitario, contenute nell'Anagrafe Regionale Operatori. Negli ultimi tre casi, è necessario inizialmente ricercare l'operatore all'interno del sistema, utilizzando, ad esempio, alcuni dei seguenti campi:

- Codice Individuale Operatore
- Codice fiscale
- Nome
- Cognome
- Data di nascita
- Comune di nascita
- Indirizzo di residenza
- Azienda di assistenza
- Azienda di appartenenza
- Codice CNS[8]

Eventuali variazioni anagrafiche devono essere notificate al Registro Variazioni. Lo Use Case *CRUD Informazioni Operatore* raggruppa gli Use Case elementari che modellano *tutte* le operazioni che possono essere eseguite su un'unità informativa, ovvero, la sua creazione, lettura, aggiornamento e cancellazione. L'acronimo CRUD sta infatti per "Create, Read, Update, Delete".

[8] Il sistema deve essere predisposto per l'utilizzo della CNS.

Extension Points

Tale Use case è esteso dallo Use Case "Notifica ad ASL di Provenienza" quando è rispettata la condizione "l'operatore cambia ASL". (Ricade in tale condizione il caso in cui l'operatore sanitario decede o va in pensione).

Precondizioni

L'attore che accede al sistema deve essere autenticato.

Postcondizioni

L'attore effettua l'operazione CRUD.

Attori

1. (Sistema di) Anagrafe Prescrittori ASL
2. (Sistema di) Registro Variazioni

Note implementative

- Qualora l'operatore non sia identificato in maniera univoca, verranno mostrate al richiedente le ricorrenze trovate, con l'indicazione dei dati anagrafici sopra elencati per la ricerca, tra le quali verrà selezionata quella di interesse.

7.2.4 Use Case Notifica ad ASL di Provenienza

Descrizione

Il servizio notifica alla ASL di provenienza dell'assistibile o dell'operatore, le eventuali variazioni anagrafiche che lo riguardano. Questo Use Case è realizzato dal modulo Gestore Eventi presentato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico.*

Precondizioni

Un assistibile o un operatore sanitario cambiano ASL, a seguito di un aggiornamento anagrafico.

Postcondizioni

L'ASL di provenienza riceve le notifiche.

Attori

Tutti e soli quelli degli Use Case CRUD Informazioni Assistibile e CRUD Informazioni Operatore.

7.2.5 Use Case Notifica Scelta MMG/PLS

Descrizione

Il servizio notifica al Registro Variazioni la scelta del MMG/PLS. Questo Use Case è realizzato dal modulo Gestore Eventi illustrato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico*.

Precondizioni

Il (Sistema di) Anagrafe Sanitaria Assistibili dell'ASL è autenticato nel sistema e un assistibile ha scelto il suo MMG/PLS.

Postcondizioni

Il Registro Variazioni riceve la notifica.

Attori

1. (Sistema di) Anagrafe Sanitaria Assistibili ASL
2. (Sistema di) Registro Variazioni

7.2.6 Use Case Notifica Revoca MMG/PLS

Descrizione

Il servizio notifica al Registro Variazioni la revoca del MMG/PLS inizialmente scelto. Questo Use Case è realizzato dal modulo Gestore Eventi illustrato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico*.

Precondizioni

Il (Sistema di) Anagrafe Sanitaria Assistibili dell'ASL è autenticato nel sistema e un assistito ha revocato il suo MMG/PLS.

Postcondizioni

Il Registro Variazioni riceve la notifica.

Attori

1. (Sistema di) Anagrafe Sanitaria Assistibili ASL
2. (Sistema di) Registro Variazioni

7.3 Anagrafe ASL (Livello Locale)

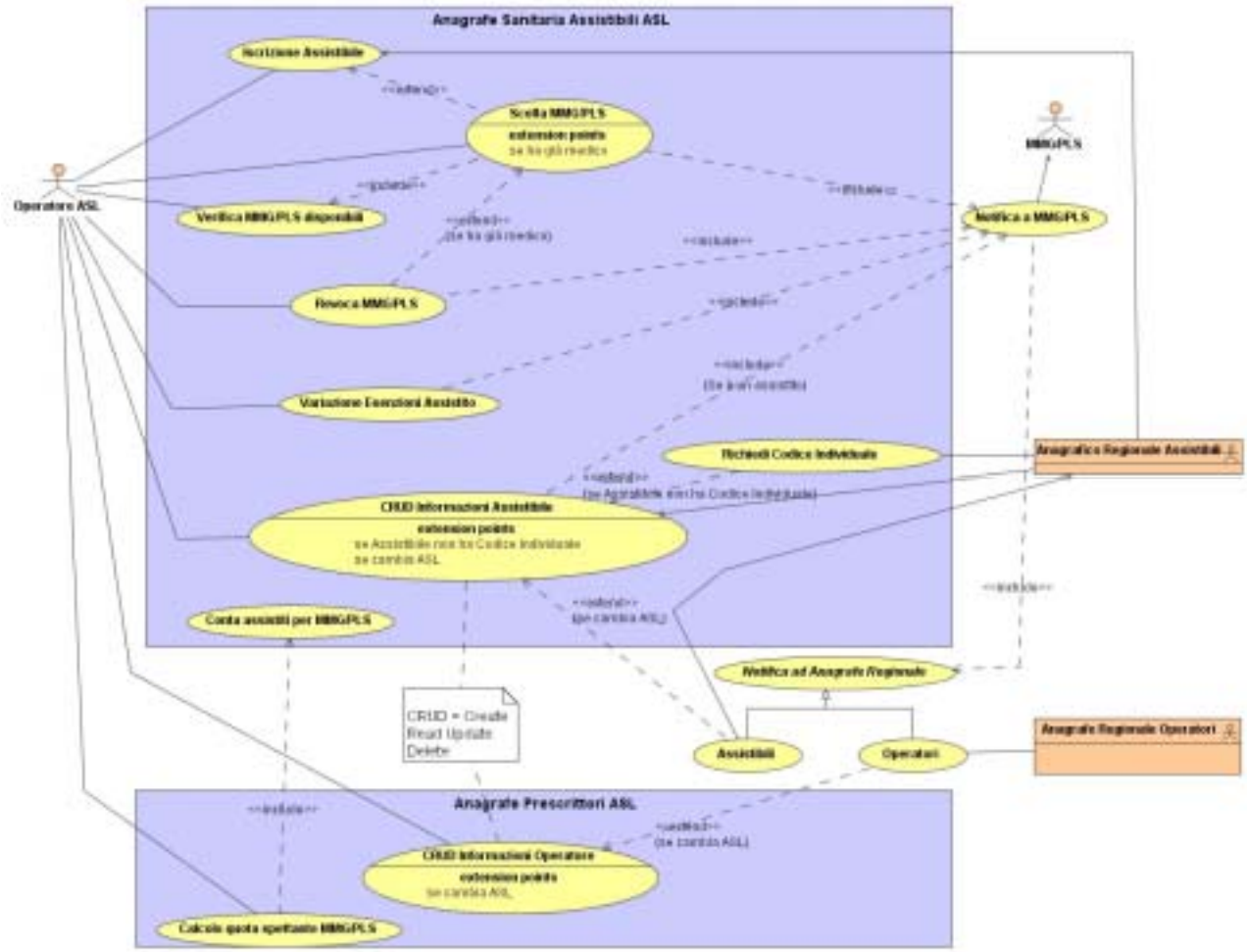


Figura 9 Sistema di Anagrafe ASL

Gli Use Case Package della Figura 9 modellano i servizi che il sistema anagrafico (prescrittori e assistibili) di una ASL fornisce al sistema di anagrafe (operatori e assistibili) regionale. Si noti, infine, che gli Use Case esterni ai due Package sono realizzati dal Gestore Eventi illustrato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico*.

Relazioni
Association [Operatore ASL – Iscrizione Assistibile]
Association [Operatore ASL – Scelta MMG/PLS]
Association [Operatore ASL – Verifica MMG/PLS disponibili]
Association [Operatore ASL - Revoca MMG/PLS]
Association [Operatore ASL – Variazione Esenzioni Assistito]
Association [Operatore ASL – CRUD Informazioni Assistibile]
Association [Anagrafico Regionale Assistibili – Richiedi Codice Individuale]

Association [Anagrafico Regionale Assistibili - CRUD Informazioni Assistibile]
Association [Operatore ASL - CRUD Informazioni Operatore]
Association [Operatore ASL – Calcolo Quota Spettante MMG/PLS]
Association [Notifica a MMG/PLS – MMG/PLS]
Association [Assistibili – Anagrafico Regionale Assistibili]
Association [Operatori – Anagrafe Regionale Operatori]
Association [Anagrafico Regionale Assistibili – Iscrizione Assistibile]
Extend [Scelta MMG/PLS – Iscrizione Assistibile]
Extend [Revoca MMG/PLS - Scelta MMG/PLS]
Extend [Richiedi Codice Individuale – CRUD Informazioni Assistibile]
Extend [Assistibili - CRUD Informazioni Assistibile]
Extend [Operatori – CRUD Informazioni Assistibile]
Include [Scelta MMG/PLS – Verifica MMG/PLS disponibili]
Include [Revoca MMG/PLS – Notifica a MMG/PLS]
Include [Variazione Esenzioni Assistito – Notifica a MMG/PLS]
Include [CRUD Informazioni Assistibile – Notifica a MMG/PLS]
Include [Calcolo Quota Spettante MMG/PLS – Conta Assistiti per MMG/PLS]
Include [Notifica a MMG/PLS – Notifica ad Anagrafe Regionale]
Include [Scelta MMG/PLS – Notifica a MMG/PLS]

7.3.1 Use Case Verifica MMG/PLS disponibili

Descrizione

Il servizio verifica quali MMG/PLS sono disponibili a ricevere un nuovo assistito.

Precondizioni

L'operatore ASL è autenticato nel sistema.

Postcondizioni

L'operatore ASL verifica gli MMG/PLS disponibili.

Attori

1. Operatore ASL

7.3.2 Use Case Scelta MMG/PLS

Descrizione

Il servizio permette di scegliere un MMG/PLS e assegnarlo ad un assistibile, che diventa, così un assistito. L'MMG/PLS deve essere scelto tra quelli disponibili a ricevere un nuovo paziente, pertanto questo Use Case include lo Use Case "Verifica MMG/PLS disponibili". Infine, l'MMG/PLS prescelto,

deve ricevere una notifica dell'avvenuto inserimento di un nuovo paziente nella lista dei suoi assistiti (cfr. relazione Include tra "Scelta MMG/PLS" e "Notifica a MMG/PLS").

Extension Points

Tale Use case è esteso dallo Use Case "Revoca MMG/PLS" quando è rispettata la condizione "l'assistibile ha già un medico". Inoltre, può estendere lo Use Case "Iscrizione Assistibile", quando, contestualmente all'iscrizione di un cittadino nell'anagrafe assistibili di una ASL, questi vuole scegliere il suo MMG/PLS.

Precondizioni

L'operatore dell'ASL è autenticato nel sistema e vi sono MMG/PLS disponibili.

Postcondizioni

L'assistibile è associato ad un MMG/PLS, il quale viene notificato di ciò. L'assistibile diventa assistito.

Attori

1. Operatore ASL

7.3.3 Use Case Revoca MMG/PLS

Descrizione

Il servizio revoca il MMG/PLS associato ad un assistito. Questo Use Case estende "Scelta MMG/PLS" quando la condizione "l'assistibile ha già un medico" è verificata. Inoltre, include lo Use Case "Notifica a MMG/PLS" in quanto il MMG/PLS riceve una notifica della revoca.

Precondizioni

L'operatore dell'ASL è autenticato nel sistema e l'assistibile ha un MMG/PLS (è un assistito).

Postcondizioni

All'assistito viene revocato il MMG/PLS, il quale viene notificato di ciò.

Attori

1. Operatore ASL

7.3.4 Use Case Iscrizione Assistibile

Descrizione

Il servizio permette di registrare un cittadino nell'anagrafe sanitaria assistibili dell'ASL.

Precondizioni

L'attore è autenticato nel sistema e il cittadino non è già registrato nell'anagrafe sanitaria assistibili dell'ASL.

Postcondizioni

Il cittadino viene registrato nell'anagrafe sanitaria assistibili dell'ASL

Attori

1. Operatore ASL
2. (Sistema di) Anagrafico Regionale Assistibili

7.3.5 Use Case Variazione Esenzioni Assistito

Descrizione

Il servizio permette di memorizzare i dati relativi all'esenzione dell'assistito.

Precondizioni

L'operatore ASL è autenticato sul sistema e il cittadino è un assistito.

Postcondizioni

I dati relativi all'esenzione dell'assistito sono aggiornati.

Attori

1. Operatore ASL

7.3.6 Use Case Notifica a MMG/PLS

Descrizione

Il servizio notifica al MMG/PLS vari aggiornamenti relativi ai suoi assistiti, riguardanti la scelta/revoca del medico, modifiche nei dati anagrafico-sanitari degli assistiti (cfr. relazioni include con gli Use Case "Scelta MMG/PLS," "Revoca MMG/PLS", "Variazione Esenzioni Assistito", "CRUD Informazioni Assistibile" (se l'assistibile è un assistito), "Notifica ad Anagrafico Regionale"). Questo Use Case è realizzato dal modulo Gestore Eventi illustrato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico*.

Precondizioni

Vi sono aggiornamenti riguardanti gli assistiti del MMG/PLS.

Postcondizioni

Il MMG/PLS riceve le notifiche relative agli aggiornamenti.

Attori

Tutti gli attori degli Use Case "Scelta MMG/PLS", "Revoca MMG/PLS", "Variazione Esenzioni Assistito", "CRUD Informazioni Assistito" (se l'assistibile è un assistito), "Notifica ad Anagrafico Regionale", ed in più:

1. MMG/PLS

7.3.7 Use Case CRUD Informazioni Assistibile

Descrizione

Il servizio permette di creare, modificare, leggere o cancellare le informazioni anagrafiche di un assistibile, contenute nell'Anagrafe sanitaria assistibili dell'ASL. Negli ultimi tre casi, è necessario inizialmente ricercare l'assistibile all'interno del sistema, utilizzando, ad esempio, alcuni dei seguenti campi:

- Codice fiscale o Codice Individuale Assistito (provvisorio, fornito quando l'assistito non è ancora in possesso del codice fiscale)
- Nome
- Cognome
- Data di nascita
- Comune di nascita
- Indirizzo di residenza
- Azienda di assistenza
- Azienda di appartenenza
- Codice CNS[9]

Eventuali variazioni anagrafiche relative ad *assistiti* devono essere notificate al MMG/PLS (cfr relazione Include tra il presente Use Case e "Notifica a MMG/PLS"). Lo Use Case *CRUD Informazioni Assistibile* raggruppa gli Use Case elementari che modellano *tutte* le operazioni che possono essere eseguite su un'unità informativa, ovvero, la sua creazione, lettura, aggiornamento e cancellazione. L'acronimo CRUD sta infatti per "Create, Read, Update, Delete".

Extension Points

Tale Use case è esteso dagli Use Case "Richiedi Codice Individuale" e "Assistibili" (figlio dello Use Case Astratto "Notifica ad Anagrafico Regionale") quando sono rispettate, rispettivamente, le condizioni seguenti:

- l'assistibile non ha Codice Individuale
- l'assistibile cambia ASL

[9] Il sistema deve essere predisposto per l'utilizzo della CNS.

Precondizioni

L'attore che accede al sistema deve essere autenticato. Inoltre, nel caso di accesso in lettura, aggiornamento o cancellazione, il cittadino deve essere un assistibile (deve esistere nell'anagrafe dell'ASL il record ad esso relativo).

Postcondizioni

L'attore effettua l'operazione CRUD.

Attori

1. Operatore ASL
2. (Sistema di) Anagrafico Regionale Assistibili

Note implementative

- Qualora l'assistibile non sia identificato in maniera univoca, verranno mostrate al richiedente le ricorrenze trovate, con l'indicazione dei dati anagrafici sopra elencati per la ricerca, tra le quali verrà selezionata quella di interesse.

7.3.8 Use Case Richiedi Codice Individuale

Descrizione

Il servizio permette di creare un Codice Individuale (univoco e provvisorio) per un assistibile che ne è sprovvisto. Questo Use Case estende lo Use Case "CRUD Informazioni Assistibile" quando la condizione "l'assistibile non ha Codice Individuale".

Precondizioni

L'attore è autenticato sul sistema e l'assistibile non ha Codice Fiscale (né Codice Individuale sanitario).

Postcondizioni

L'assistibile è associato con un Codice Individuale Sanitario che permette di identificarlo in maniera univoca.

Attori

Tutti gli attori dello Use Case "CRUD Informazioni Assistibile" ed in più:

1. (Sistema di) Anagrafico Regionale Assistibili

7.3.9 Use Case Conta Assistiti

Descrizione

Il servizio permette di contare il numero di assistiti di un MMG/PLS. Questo numero è necessario per calcolare la quota spettante a MMG/PLS (cfr. relazione include tra lo Use Case "Calcolo quota spettante MMG/PLS" e il presente).

Precondizioni

Nessuna.

Postcondizioni

Viene calcolato il numero di assistiti del medico.

Attori

Tutti e soli quelli dello Use Case "Calcolo quota spettante MMG/PLS"

7.3.10 Use Case Calcolo Quota Spettante MMG/PLS

Descrizione

Il servizio calcola il quantitativo da pagare al MMG/PLS, sulla base del numero dei suoi assistiti.

Precondizioni

Il MMG/PLS è registrato nell'anagrafe prescrittori dell'ASL.

Postcondizioni

Viene calcolato il corrispettivo da pagare al MMG/PLS.

Attori

1. Operatore ASL

7.3.11 Use Case Notifica CRUD Informazioni Operatore

Descrizione

Il servizio permette di creare, modificare, leggere o cancellare le informazioni anagrafiche di un operatore sanitario, contenute nell'Anagrafe Prescrittori ASL (oppure nell'Anagrafe Regionale Operatori, se l'operatore sanitario non è un prescrittore[10]). Negli ultimi tre casi, è necessario inizialmente ricercare l'operatore all'interno del sistema, utilizzando, ad esempio, alcuni dei seguenti campi:

- Codice Individuale Operatore
- Codice fiscale
- Nome
- Cognome
- Data di nascita
- Comune di nascita
- Indirizzo di residenza
- Azienda di assistenza
- Azienda di appartenenza
- Codice CNS[11]

Eventuali variazioni anagrafiche devono essere notificate all'Anagrafe Regionale Operatori (cf. relazione di estensione descritta sotto). Lo Use Case *CRUD Informazioni Operatore* raggruppa gli Use Case elementari che modellano *tutte* le operazioni che possono essere eseguite su un'unità informativa, ovvero, la sua creazione, lettura, aggiornamento e cancellazione. L'acronimo CRUD sta infatti per "Create, Read, Update, Delete".

Extension Points

Tale Use case è esteso dallo Use Case "Operatori" (figlio dello Use Case Astratto "Notifica ad Anagrafe Regionale") quando è rispettata la condizione "l'operatore cambia ASL" (Ricade in tale condizione il caso in cui l'operatore sanitario decede o va in pensione).

Precondizioni

L'attore che accede al sistema deve essere autenticato.

Postcondizioni

L'attore effettua l'operazione CRUD.

Attori

1. Operatore ASL

Note implementative

- Qualora l'operatore non sia identificato in maniera univoca, verranno mostrate al richiedente le ricorrenze trovate, con l'indicazione dei dati anagrafici sopra elencati per la ricerca, tra le quali verrà selezionata quella di interesse.

[10] Questo secondo caso non è mostrato in figura 9.
[11] Il sistema deve essere predisposto per l'utilizzo della CNS.

7.3.12 Use Case Notifica ad Anagrafe Regionale

Descrizione

Questo Use Case *astratto* modella le notifiche che gli anagrafici regionali (assistibili e operatori) ricevono, ed in particolare, tutte quelle ricevute dal MMG/PLS (cfr. relazione di inclusione tra lo Use Case "Notifica a MMG/PLS" e il presente Use Case). Questo Use Case è realizzato dal modulo Gestore Eventi illustrato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico*.

Use Case Figli

1. Assistibili
2. Operatori

7.3.13 Use Case Assistibili

Descrizione

Il servizio permette di notificare all'Anagrafica Regionale Assistibili gli aggiornamenti anagrafici riguardanti gli assistibili, in particolare, se gli assistibili cambiano ASL (cfr. relazione di estensione tra questo Use Case e lo Use case "CRUD Informazioni Assistibili"). Questo Use Case è realizzato dal modulo Gestore Eventi illustrato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico*.

Precondizioni

Vi è una variazione anagrafica di un assistibile.

Postcondizioni

L'Anagrafica Regionale Assistibili riceve la notifica.

Attori

Tutti gli attori degli Use Case "Notifica a MMG/PLS" e "CRUD Informazioni Assistibili"

1. (Sistema di) Anagrafico Regionale Assistibili

7.3.14 Use Case Operatori

Descrizione

Il servizio permette di notificare all'Anagrafe Regionale Operatori gli aggiornamenti anagrafici riguardanti gli operatori sanitari, in particolare, se gli operatori cambiano ASL (cfr. relazione di estensione tra questo Use Case e lo Use case "CRUD Informazioni Operatore"). Questo Use Case è realizzato dal modulo Gestore Eventi illustrato nella Sezione *Registro Variazioni* dell'*Allegato E - Capitolato Tecnico*.

Precondizioni

Vi è una variazione anagrafica di un operatore sanitario.

Postcondizioni

L'Anagrafe Regionale Operatori riceve la notifica.

Attori

Tutti gli attori degli Use Case "Notifica a MMG/PLS" e "CRUD Informazioni Operatore"

1. (Sistema di) Anagrafe Regionale Operatori

8 SERVIZI DI RETE MMG

In questa sezione vengono modellati i servizi funzionali che il sistema (integrato regionale) deve offrire ai Medici di Medicina Generale e ai Pediatri di Libera Scelta e agli altri operatori sanitari coinvolti.

Nella Sezione 8.1 viene introdotta la lista completa degli attori (ruoli) coinvolti nei diagrammi che modellano i servizi e che sono presentati successivamente. Nelle Sezioni 8.2 e 8.3 vengono modellati con UML Activity Diagram alcuni i processi significativi per il progetto in esame[12], ed in particolare:

- Farmaceutica convenzionata
- Prestazione specialistica, ambulatoriale o di diagnostica

La Sezione 0 introduce le relazioni tra gli Activity Diagram e gli Use Case di interesse, mediante una matrice: tali relazioni sono poi riprese e discusse nelle Sezioni 8.5 – 8.11, mediante un'analisi dettagliata degli Use Case. In fase di progettazione esecutiva tale modello dovrà essere, ovviamente, contestualizzato e dettagliato. In particolare, il modello di Use Case presentato qui va inteso come un insieme di requisiti minimi e non esaurisce lo scenario d'uso del sistema. Il Fornitore dovrà infatti provvedere all'approfondimento e al completamento di tali requisiti come parte del lavoro di progettazione. Delle specifiche va fornito il modello UML 2.0[13] in formato XMI (OMG Xml Metadata Interchange) e nell'eventuale formato proprietario dello strumento di modellazione concordato all'inizio del progetto. La specifica dovrà comprendere inoltre un documento testuale in formato .rtf e .pdf.

8.1 Attori

Gli attori coinvolti negli Activity Diagram e negli Use Case sono i seguenti:

1. (Sistema di) Anagrafe Sanitaria Regionale
2. Assistito
3. Prenotatore
4. *Operatore di Accettazione* (attore astratto)
    a. Operatore di Accettazione Ambulatoriale (amm.vo)
5. *Operatore Sanitario*[14] (attore astratto)
    a. *Prescrittore* (attore astratto)
        i. Erogatore
        ii. MMG/PLS
6. Farmacia
7. ASL/Regione

8.2 Activity Diagram Farmaceutica Convenzionata

L'Activity Diagram in Figura 10 modella l'*attuale* processo sanitario/amministrativo per giungere all'erogazione dei farmaci di fascia C (con prescrizione obbligatoria), cioè *in assenza* dell'infrastruttura informatica necessaria all'interoperabilità tra i diversi attori. Nelle note in giallo vengono brevemente elencati i servizi di integrazione previsti.

[12] I processi di disegnati tramite Activity Diagram UML sono *ex-ante*, sono cioè i processi di alto livello come si svolgono attualmente, senza l'implementazione della rete MMG/PLS, gli Use Case rappresentano invece una prima specifica del comportamento del sistema.

[13] Vedi: http://www.uml.org.

[14] Si noti che nel seguito del documento, con il termine "Operatore Sanitario" ci si riferisce agli operatori sanitari propriamente detti (medici, infermieri, capo reparti, ecc.), mentre con il termine "Operatore" ci si riferisce, più in generale, a tutti gli utenti del sistema (quindi anche ad altre figure professionali quali ad esempio: prenotatori, operatori di accettazione, ecc.)

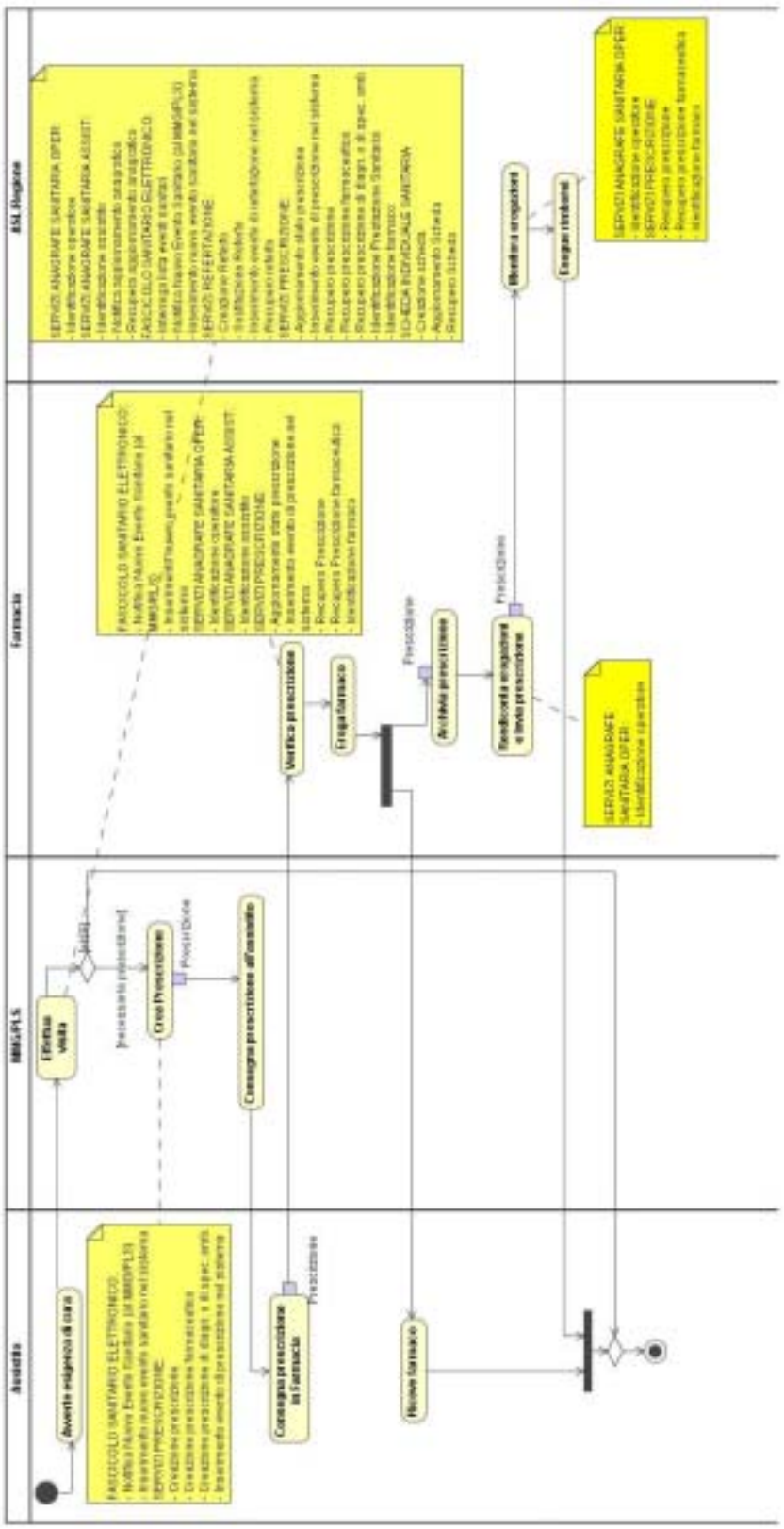


Figura 10. Farmaceutica Convenzionata

8.3 Activity Diagram Prestazione Specialistica Ambulatoriale o di Diagnostica

L'Activity Diagram in Figura 11 modella l'*attuale* processo sanitario/amministrativo per giungere all'erogazione di una prestazione specialistica, cioè *in assenza* dell'infrastruttura informatica necessaria all'interoperabilità tra i diversi attori. Nelle note in giallo vengono brevemente elencati i servizi di integrazione previsti, rappresentati nel modello degli Use Case (Sezione 8.6 e successive)

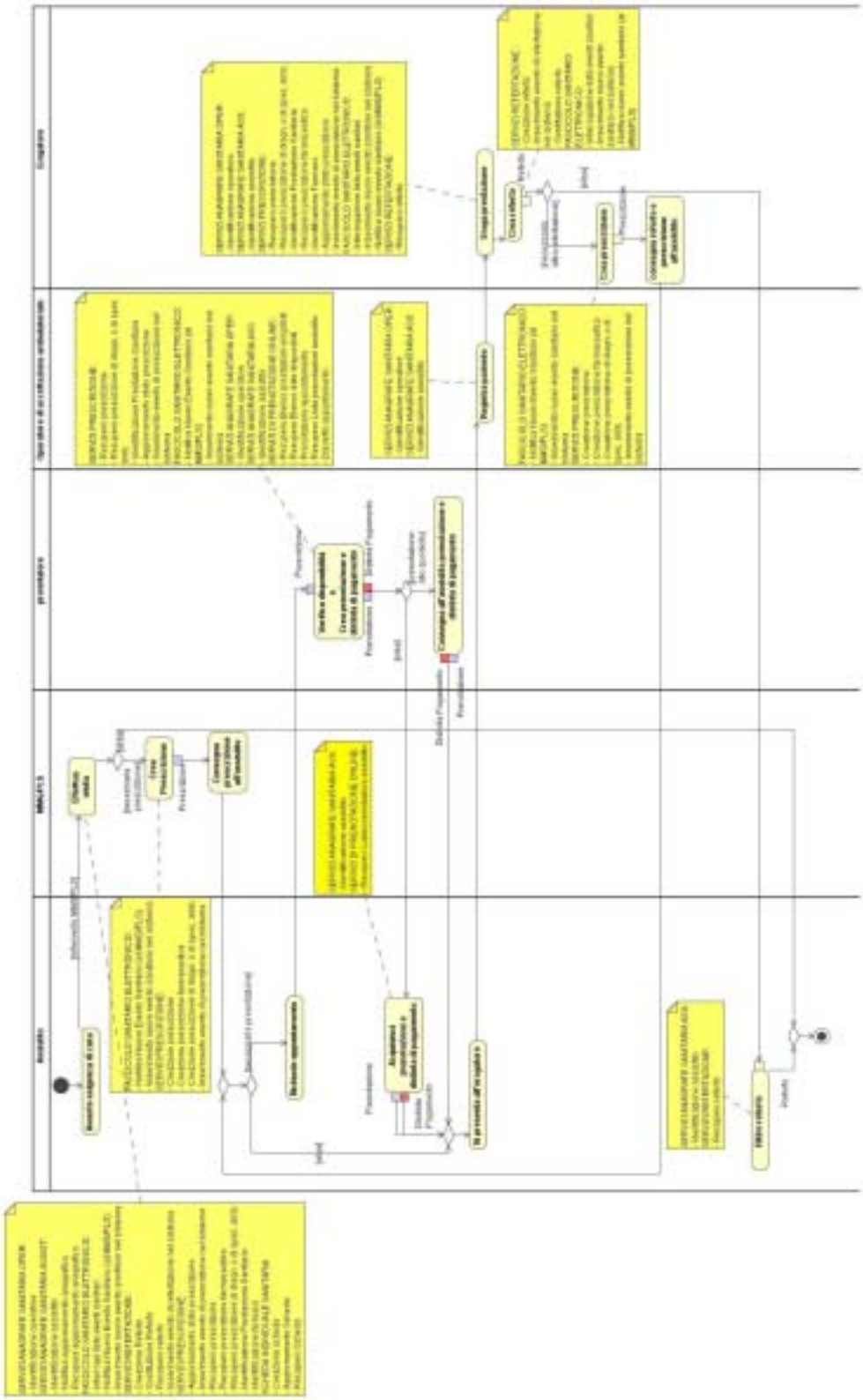


Figura 11: Prestazione Specialistica, Ambulatoriale o di Diagnostica

8.4 Matrice introduttiva delle relazioni tra Activity Diagram e Use Case

Le matrici seguenti presentano una vista globale delle relazioni tra gli Activity Diagram presentati nelle sezioni precedenti e gli Use Case che verranno introdotti successivamente. In particolare, nelle colonne sono indicati, per ciascun Activity Diagram, le attività che possono godere dei benefici derivanti dalla sanità elettronica; nelle righe sono indicati gli Use Case di interesse (si ricorda che l'informazione su quali Use Case sono di interesse per quale attività è anche contenuta nelle note in giallo presenti negli Activity Diagram); nelle celle sono indicati gli attori coinvolti negli Use Case che interessano le attività degli Activity Diagram. Ad esempio, si consideri l'attività Effettua Visita (eseguita dal MMG/PLS) dell'Activity Diagram Farmaceutica Convenzionata: per essere correttamente eseguita nell'ambito della sanità elettronica, essa avrà necessità di usufruire del servizio Identificazione Assistito.

		Farmaceutica convenzionata				
		Effettua visita	Crea Prescrizione	Verifica Prescrizione	Rendiconta erogazioni e invia prescrizioni	Monitora Erogazioni
Servizi Anagrafe Sanitaria Assistiti	Identificazione Assistito	MMG/PLS		Farmacia		
	Trasmissione Aggiornamenti					
	Notifica Aggiornamento	MMG/PLS				
	Recupero Aggiornamento	MMG/PLS				
Servizi Anagrafe Operatori	Identificazione Operatore Sanitario	MMG/PLS		Farmacia	Farmacia	ASL/Regione
Servizi Prescrizione	Creazione Prescrizione		MMG/PLS			
	Creazione Prescrizione Farmaceutica		MMG/PLS			
	Creazione Prescrizione ambulatoriale, specialistica e di diagnostica, o di rivovero		MMG/PLS			
	Aggiornamento stato prescrizione	MMG/PLS		Farmacia		
	Inserimento evento di prescrizione nel sistema	MMG/PLS	MMG/PLS	Farmacia		
	Recupero Prescrizione	MMG/PLS		Farmacia		ASL/Regione
	Recupero Prescrizione Farmaceutica	MMG/PLS		Farmacia		ASL/Regione
	Recupero Prescrizione specialistica ambulatoriale o di diagnostica, o di ricovero	MMG/PLS				
	Identificazione Prestazione Sanitaria	MMG/PLS				
	Identificazione Farmaco	MMG/PLS		Farmacia		ASL/Regione
Servizi Refertazione	Creazione Referto	MMG/PLS				
	Sostituzione Referto	MMG/PLS				
	Inserimento Evento di refertazione nel sistema	MMG/PLS				
	Recupero Referto	MMG/PLS				
Servizi di Prenotazione online	Recupero Elenco Prestazioni Erogabili					
	Recupero Elenco Date Disponibili					
	Prenotazione Appuntamento					
	Recupero Lista Prenotazioni Assistito					
	Disdetta Appuntamento					
Servizi Fascicolo Sanitario Elettronico	Interrogazione lista eventi sanitari	MMG/PLS				
	Inserimento nuovo evento nel sistema	MMG/PLS	MMG/PLS	Farmacia		
	Notifica nuovo evento sanitario (al MMG/PLS)	MMG/PLS	MMG/PLS	Farmacia		
Scheda Individuale Sanitaria	Creazione Scheda	MMG/PLS				
	Aggiornamento Scheda	MMG/PLS				
	Recupero Scheda	MMG/PLS				

Tabella 1. Matrice introduttiva relazioni Activity Diagram Farmaceutica Convenzionata - Use Case

		Prestazione di Specialistica Ambulatoriale o di Diagnostica							
		Effettua visita	Crea Prescrizione	Verifica disponibilità e crea prenotazione e distinta di pagamento	Acquisisci prenotazione e distinta di pagamento	Registra Paziente	Eroga Prestazione	Crea Referto	Ritiro referto
Servizi Anagrafe Sanitaria Assistiti	Identificazione Assistito	MMG/PLS		Prenotatore	Assistito	Operatore di accettazione ambulatoriale (amm.vo)	Erogatore		Assistito
	Trasmissione Aggiornamenti								
	Notifica Aggiornamento	MMG/PLS							
	Recupero Aggiornamento	MMG/PLS							
Servizi Anagrafe Operatori	Identificazione Operatore Sanitario	MMG/PLS		Prenotatore		Operatore di accettazione ambulatoriale (amm.vo)	Erogatore		
Servizi Prescrizione	Creazione Prescrizione		MMG/PLS Erogatore						
	Creazione Prescrizione Farmaceutica		MMG/PLS Erogatore						
	Creazione Prescrizione ambulatoriale, specialistica e di diagnostica, o di rivovero		MMG/PLS Erogatore						
	Aggiornamento stato prescrizione	MMG/PLS		Prenotatore			Erogatore		
	Inserimento evento di prescrizione nel sistema	MMG/PLS	MMG/PLS Erogatore	Prenotatore			Erogatore		
	Recupero Prescrizione	MMG/PLS		Prenotatore			Erogatore		
	Recupero Prescrizione Farmaceutica	MMG/PLS					Erogatore		
	Recupero Prescrizione specialistica ambulatoriale o di diagnostica, o di ricovero	MMG/PLS		Prenotatore			Erogatore		
	Identificazione Prestazione Sanitaria	MMG/PLS		Prenotatore			Erogatore		
	Identificazione Farmaco	MMG/PLS					Erogatore		
Servizi Refertazione	Creazione Referto	MMG/PLS						Erogatore	
	Sostituzione Referto	MMG/PLS						Erogatore	
	Inserimento Evento di refertazione nel sistema	MMG/PLS						Erogatore	
	Recupero Referto	MMG/PLS					Erogatore		Assistito
Servizi di Prenotazione online	Recupero Elenco Prestazioni Erogabili			Prenotatore					
	Recupero Elenco Date Disponibili			Prenotatore					
	Prenotazione Appuntamento			Prenotatore					
	Recupero Lista Prenotazioni Assistito			Prenotatore	Assistito				
	Disdetta Appuntamento			Prenotatore					
Servizi Fascicolo Sanitario Elettronico	Interrogazione lista eventi sanitari	MMG/PLS					Erogatore	Erogatore	
	Inserimento nuovo evento nel sistema	MMG/PLS	MMG/PLS Erogatore	Prenotatore			Erogatore	Erogatore	
	Notifica nuovo evento sanitario (al MMG/PLS)	MMG/PLS	MMG/PLS Erogatore	Prenotatore			Erogatore	Erogatore	
Scheda Individuale Sanitaria	Creazione Scheda	MMG/PLS							
	Aggiornamento Scheda	MMG/PLS							
	Recupero Scheda	MMG/PLS							

Tabella 2. Matrice introduttiva relazioni Activity Diagram Prestazione di Specialistica Ambulatoriale o di Diagnostica - Use Case

8.5 Use Case: Aspetti implementativi comuni

Ciascun servizio identificato da uno Use Case può essere invocato e visualizzato mediante:

- interfaccia alla porta delegata (cf. specifiche SPCC – CNIPA)
- interfaccia html (browser web)

8.6 Use Case Package Anagrafe Sanitaria Assistiti

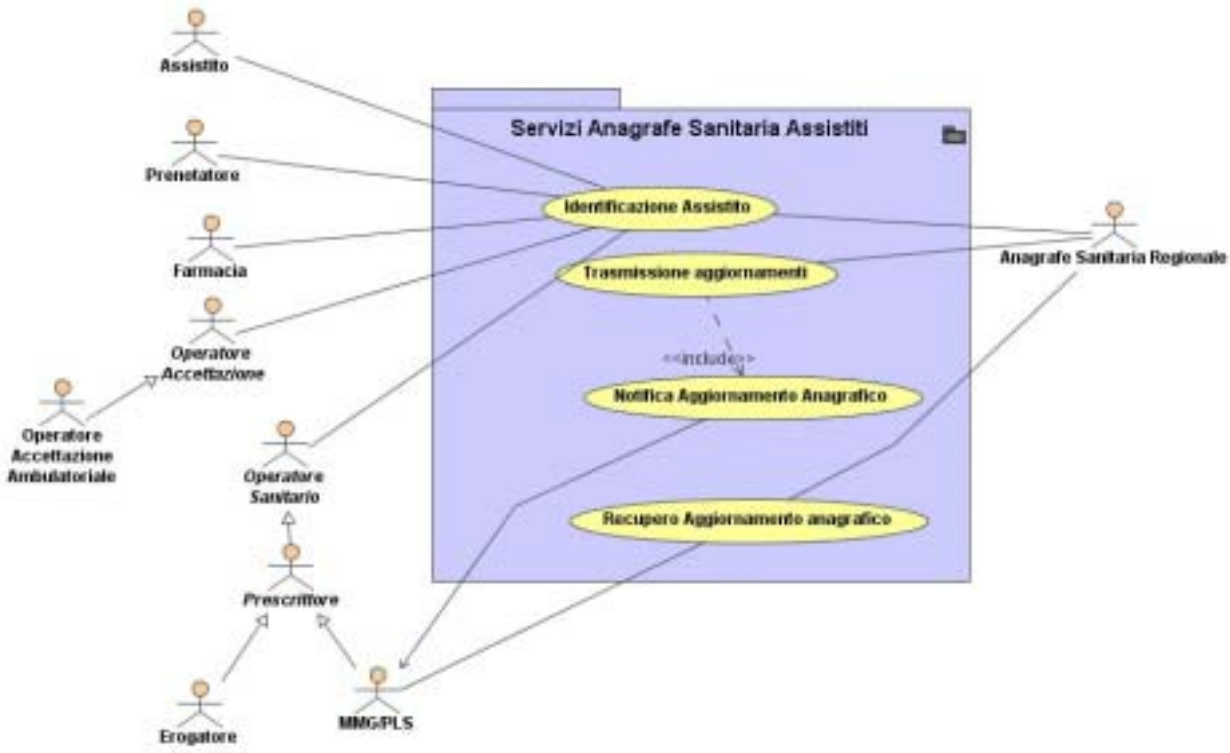


Figura 12. Servizi Anagrafe Assistiti

Fornisce servizi dell'anagrafe sanitaria agli attori del sistema permettendo di identificare gli assistiti e di fornire alcune informazioni amministrative (es. scelta/revoca MMG/PLS[15], esenzioni, vaccinazioni). Si noti che per la semantica di <<include>> ogni volta che viene trasmesso un aggiornamento, esso viene anche notificato al medico. Tuttavia, si è anche indicata in modo esplicito l'associazione tra l'attore e l' "included" use case, poiché in determinate circostanze può essere lo stesso medico a trasmettere al sistema un aggiornamento relativo ad un assistito (nei due casi il verso di navigazione dell'associazione attore-use case è diverso).

Relazioni interne
Association [Assistito - Identificazione Assistito]
Association [Prenotatore - Identificazione Assistito]
Association [Farmacia - Identificazione Assistito]
Association [Operatore Accettazione - Identificazione Assistito]
Association [Operatore Sanitario - Identificazione Assistito]

[15] Si assume l'esistenza di un servizio di scelta e revoca.

Association [MMG/PLS - Recupero Aggiornamento anagrafico]
Association [Notifica Aggiornamento Anagrafico - MMG/PLS]
Association [Anagrafe Sanitaria Regionale - Recupero Aggiornamento anagrafico]
Association [Anagrafe Sanitaria Regionale - Trasmissione aggiornamenti]
Association [Anagrafe Sanitaria Regionale - Identificazione Assistito]
Include [Trasmissione aggiornamenti - Notifica Aggiornamento Anagrafico]

8.6.1 Use Case Identificazione Assistito

Descrizione

Il servizio ha lo scopo di identificare l'assistito all'interno del sistema sanitario regionale, di identificarne le informazioni anagrafiche e le informazioni relative al suo MMG/PLS ed alle eventuali esenzioni per patologie o invalidità. Vengono trasmessi anche i dati sul consenso.

Le responsabilità del servizio sono le seguenti:

- Identificare l'assistito
- Identificare il tipo di esenzioni alla spesa sanitaria
- Identificare i dati relativi al MMG/PLS dell'assistito

La ricerca può avvenire utilizzando alcuni fra i seguenti campi:

- Codice fiscale
- Nome
- Cognome
- Data di nascita
- Comune di nascita
- Indirizzo di residenza
- Azienda di assistenza
- Azienda di appartenenza
- Codice CNS[16]
- ...

Precondizioni

L'attore è autenticato nel sistema e il cittadino cercato è registrato nel sistema.

Postcondizioni

L'attore riceve le informazioni richieste.

Attori

1. (Sistema di) Anagrafe Sanitaria Regionale
2. Assistito
3. Prenotatore
4. Farmacia
5. *Operatore di Accettazione*
    a. Operatore di Accettazione Ambulatoriale
6. *Operatore Sanitario*
    a. *Prescrittore*
        i. Erogatore
        ii. MMG/PLS

[16] Il sistema deve essere predisposto per l'utilizzo della CNS.

Note implementative

- Se il richiedente non è l'MMG/PLS dell'assistito non vengono trasmessi i dati riguardanti le esenzioni.
- Qualora l'assistito non sia identificato in maniera univoca, verranno mostrate al richiedente le ricorrenze trovate, con l'indicazione dei dati anagrafici sopra elencati per la ricerca, tra le quali verrà selezionata quella di interesse.

8.6.2 Use Case Trasmissione Aggiornamenti

Descrizione

Il servizio consente all'anagrafe di inviare al sistema i dati anagrafici degli assistiti a seguito di variazioni dei dati anagrafici, scelte e revoche dei medici di base. E' responsabilità del servizio permettere la trasmissione dei file contenenti gli aggiornamenti per ciascun medico del sistema e le notifiche relative agli aggiornamenti. Ogni volta che un aggiornamento viene trasmesso, viene inviata al MMG/PLS una notifica.

Attori

1. Anagrafe Sanitaria Regionale

Precondizioni

Si verifica un aggiornamento nell'anagrafe sanitaria (Variazioni anagrafiche, scelta/revoca MMG/PLS, ecc.)

Postcondizioni

Viene attivata la notifica dell'aggiornamento all'MMG/PLS.

8.6.3 Use Case Notifica Aggiornamento Anagrafico

Descrizione

Viene creata e inviata una notifica al MMG/PLS per ciascun assistito per cui si siano verificate delle variazioni anagrafiche o relative al processo di scelta/revoca.

Attori

1. MMG/PLS

PreCondizioni

E' stato ricevuto un aggiornamento anagrafico (da parte del sistema).

PostCondizioni

L'MMG/PLS coinvolto riceve la notifica.

8.6.4 Use Case Recupero Aggiornamento Anagrafico

Descrizione

Il servizio permette al medico di recuperare e caricare sul suo PC l'aggiornamento anagrafico notificato.

Attori

1. Anagrafe Sanitaria Regionale
2. MMG/PLS

PreCondizioni

Il medico ha ricevuto la notifica di un aggiornamento anagrafico.

PostCondizioni

Il medico ha recuperato l'aggiornamento anagrafico.

8.7 Use Case Package Servizi Anagrafe Operatori

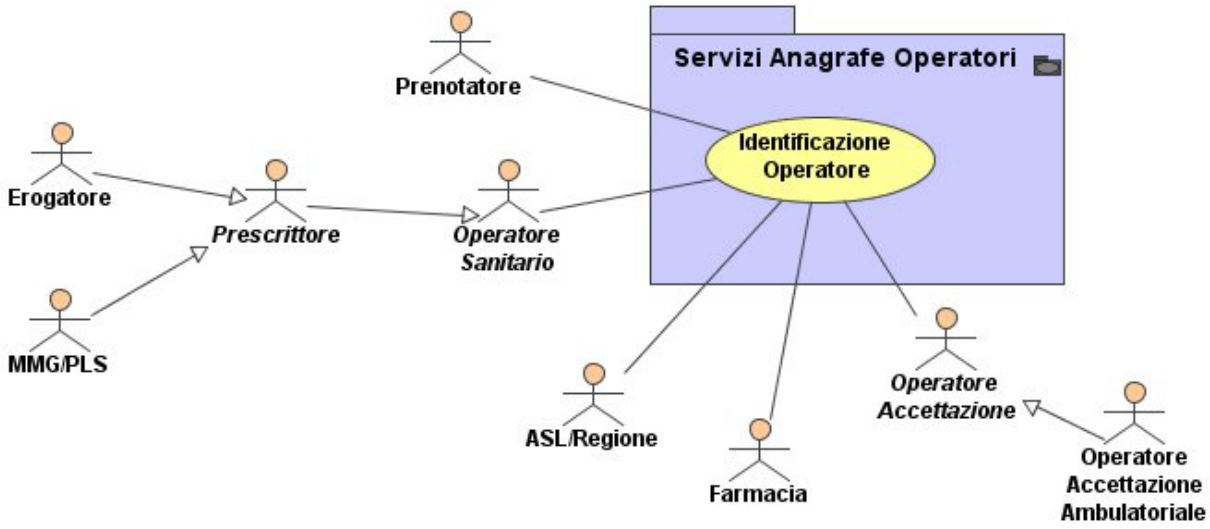


Figura 13: Servizi Anagrafe Operatori

Fornisce un servizio per l'identificazione degli operatori, intendendo con questo termine tutti coloro (personale sanitario e non) che ha accesso ai dati sensibili degli assistiti.

Relazioni Interne
Association [Prenotatore - Identificazione Operatore]
Association [Operatore Sanitario - Identificazione Operatore]
Association [ASL/Regione - Identificazione Operatore]
Association [Farmacia - Identificazione Operatore]
Association [Operatore Accettazione- Identificazione Operatore]

8.7.1 Use Case Identificazione Operatore

Descrizione

Permette l'identificazione degli operatori. Si noti che questa anagrafe non contiene solo gli operatori sanitari propriamenti detti, ma tutti coloro che devono avere accesso ai dati sensibili degli assistiti. In accordo con quanto accennato nella Sezione *Servizi applicativi della rete MMG/PLS* dell'*Allegato E - Capitolato Tecnico*, l'identificazione dell'operatore avviene tramite dispositivi di autenticazione, come ad esempio smart-card CNS.

Attori

1. Prenotatore
2. *Operatore di Accettazione*
   a. Operatore di Accettazione Ambulatoriale
3. *Operatore Sanitario*
   a. *Prescrittore*
      i. Erogatore
      ii. MMG/PLS
4. ALS/Regione
5. Farmacia

PreCondizioni
L'attore è autenticabile dal sistema
PostCondizioni
L'attore è autenticato dal sistema

8.8 Use Case Package Servizi di Prenotazione Online

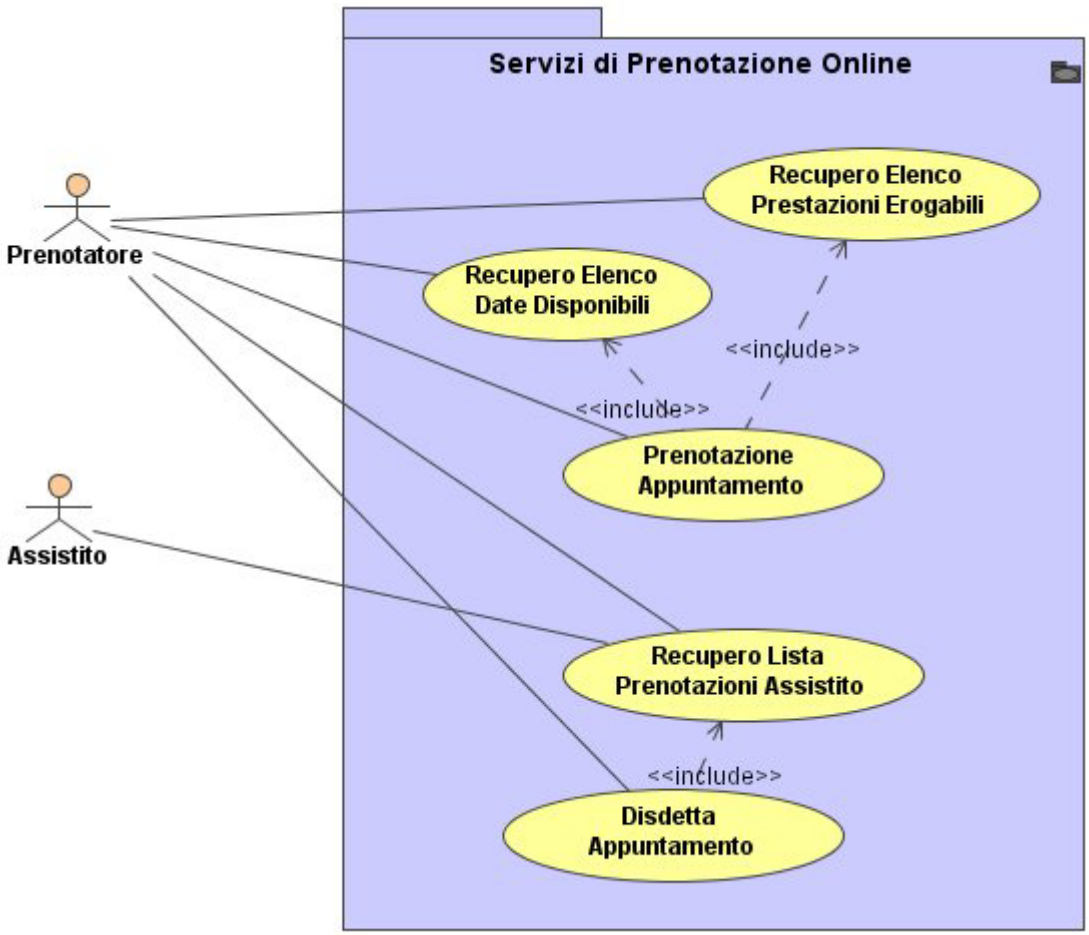


Figura 14. Servizi di Prenotazione Online

Fornisce servizi per la gestione delle prenotazioni dell'assistito.

Relazioni Interne
Association [Prenotatore - Recupero Elenco Prestazioni Erogabili]
Association [Prenotatore - Recupero Elenco Date Disponibili]
Association [Prenotatore - Prenotazione Appuntamento]
Association [Prenotatore – Recupero Lista Prenotazioni Assistito]
Association [Prenotatore - Disdetta Appuntamento]
Association [Assistito - Recupero Lista Prenotazioni Assistito]
Include [Disdetta Appuntamento - Recupero Lista Prenotazioni Assistito]
Include [Prenotazione Appuntamento - Recupero Elenco Date Disponibili]
Include [Prenotazione Appuntamento - Recupero Elenco Prestazioni Erogabili]

8.8.1 Use Case Recupero Elenco Prestazioni Erogabili

Descrizione

Il servizio restituisce l'elenco delle prestazioni erogabili da una struttura e quindi prenotabili per l'assistito.

Attori

1. Prenotatore

PreCondizioni

L'attore è identificato dal sistema.

PostCondizioni

Viene restituita la lista delle prestazioni erogabili dalla struttura

8.8.2 Use Case Recupero Elenco Date Disponibili

Descrizione

Il servizio restituisce l'elenco delle date in cui una determinata prestazione può essere erogata.

Attori

1. Prenotatore

PreCondizioni

L'attore è identificato dal sistema e la prestazione richiesta è erogata dalla struttura.

PostCondizioni

Viene restituita una lista di date disponibili in cui la prestazione richiesta può essere erogata.

8.8.3 Use Case Prenotazione Appuntamento

Descrizione

Il servizio permette di prenotare un appuntamento per l'assistito in relazione ad una data prestazione. Si noti che per la semantica di <<include>> ogni volta che viene prenotato un appuntamento, vengono recuperati gli elenchi delle date disponibili e delle prestazioni erogabili. Inoltre, in presenza di prescrizione, essa viene recuperata (cfr. associazione Prenotatore – Recupero Prescrizione nello Use Case Package Servizi Prescrizione).

Attori

1. Prenotatore

PreCondizioni

L'attore è identificato dal sistema. La prestazione richiesta dall'assistito è tra quelle erogabili dalla struttura e vi è disponibilità in un giorno accettato dall'assistito.

PostCondizioni

Viene prenotata la prestazione richiesta dall'assistito nella data concordata. Il periodo in cui la prestazione verrà erogata può essere reso non disponibile per altre prestazioni dello stesso tipo. In presenza di prescrizione, ne viene aggiornato lo stato (cfr. associazione Prenotatore – Aggiornamento stato prescrizione nello Use Case Package Servizi Prescrizione).

8.8.4 Use Case Disdetta Appuntamento

Descrizione

Viene disdetto un appuntamento prenotato. Può essere visto come un caso particolare di prenotazione di un appuntamento.

Attori

1. Prenotatore

PreCondizioni

L'attore è autenticato dal sistema. Esiste almeno una prenotazione dell'assistito ad una prestazione non ancora erogata.

PostCondizioni

Viene disdetta la prenotazione indicata (anche più d'una).

8.8.5 Use Case Recupero Lista Prenotazioni Assistito

Descrizione

L'attore ottiene la lista delle prenotazioni effettuate dall'assistito ma non ancora erogate. Si noti che questo è l'unico servizio (tra quelli di questo package di use case) invocabile dall'assistito. Inoltre, esso non modifica l'elenco delle prenotazioni. La ricerca può riguardare tutte le prenotazioni dell'assistito oppure può essere limitata a quelle relative ad un dato intervallo temporale, ad una data tipologia di prestazioni, ecc.

Attori

1. Assistito
2. Prenotatore

PreCondizioni

L'attore viene autenticato dal sistema.

PostCondizioni

Viene restituita la lista (eventualmente vuota) delle prestazioni prenotate dall'assistito, ma non ancora erogate.

8.9 Use Case Package Fascicolo Sanitario Elettronico

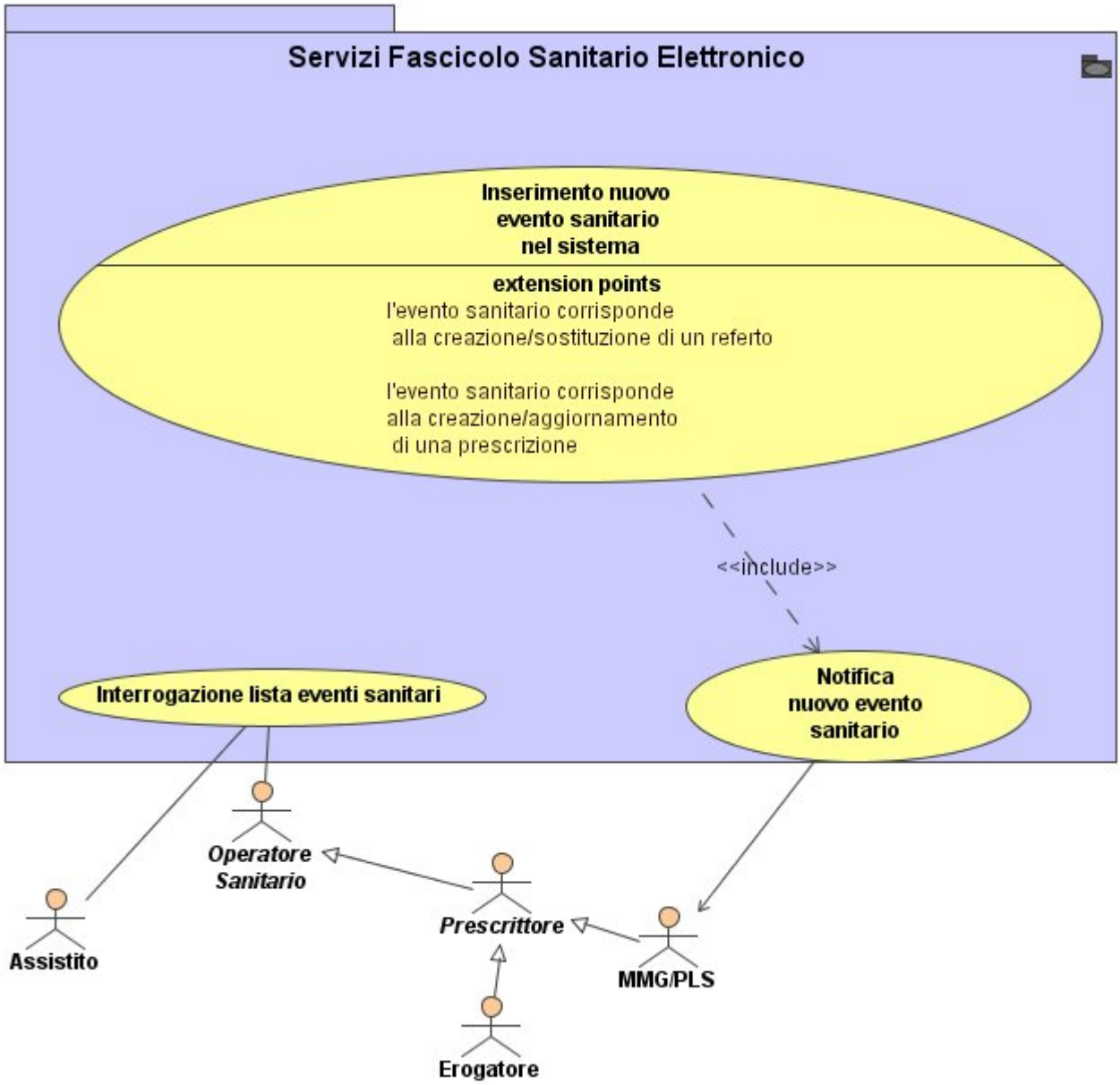


Figura 15. Fascicolo Sanitario Elettronico

Il Fascicolo Sanitario Elettronico (FSE) permette di mantenere un indice degli eventi sanitari dell'individuo (prescrizioni, referti, certificati). Questo permette al medico (autorizzato dall'assistito o in situazione di emergenza) di conoscere la storia passata del assistito e di conoscere le prescrizioni mediche che ha avuto nel passato. Il Fascicolo non contiene dati medici che rimangono nei repository originali ma permette di ritrovare, in modo trasparente, i dati.

Il meccanismo di registrazione/interrogazione degli eventi può avvenire, ad esempio, secondo il modello IHE-XDS[17], come accennato nella Sezione 3.1 *Componenti Logici dell'Architettura*. Si ricorda, tuttavia, che l'eventuale uso del profilo XDS-IHE è da considerarsi provvisorio in quanto non è in grado di supportare un FSE interoperabile a livello nazionale. Verrà sostituito da strumenti e regole tecniche realizzate nell'ambito del Tavolo permanente di Sanità Elettronica.

[17] Vedi: http://www.ihe.net/tf/IHE_ITI_Cross-enterprise_Doc_Sharing_2004_08-15.pdf

Relazioni interne
Association [Operatore Sanitario - Interrogazione lista eventi sanitari]
Association [Assistito - Interrogazione lista eventi sanitari]
Association [Notifica nuovo evento sanitario – MMG/PLS]
Include [Inserimento nuovo evento sanitario nel sistema – Notifica nuovo evento sanitario]

8.9.1 Use Case Interroga Lista Eventi Sanitari

Descrizione

Il servizio, a seguito di una richiesta, restituisce la lista degli eventi sanitari di uno specifico assistito.

Attori

1. Assistito
2. *Operatore Sanitario*
   a. *Prescrittore*
      i. Erogatore
      ii. MMG/PLS

PreCondizioni

L'attore è autenticato sul sistema.

PostCondizioni

L'attore ha ricevuto la lista di eventi sanitari richiesta.

Note implementative

I MMG/PLS possono operare solo sui propri assistiti o in base ad una specifica autorizzazione. Analogamente per gli erogatori.

8.9.2 Use Case Inserimento Nuovo Evento Sanitario nel Sistema

Descrizione

Ogni volta che viene creata una prescrizione o un referto, oppure un assistito viene ricoverato in una struttura ospedaliera o dimesso da essa, viene generato un nuovo evento sanitario e nel sistema viene inserito automaticamente (il riferimento ad) un nuovo evento sanitario[18]. Tale "automatismo" è stato reso mediante una serie di <<include>> negli Use Case Package Servizi Prescrizione e Servizi Refertazione tra gli Use Case relativi alla creazione dell'evento sanitario di competenza e lo Use Case relativo all'inserimento dell'evento sanitario nel sistema. Per quanto riguarda i primi, poiché le modalità di inserimento possono dipendere dall'evento sanitario, sono stati definiti Use Case che estendono lo Use Case Inserimento Nuovo Evento Sanitario nel Sistema. Di conseguenza, lo Use Case Inserimento Nuovo Evento Sanitario nel Sistema non è associato a nessun attore esterno al sistema, ma rappresenta una funzionalità interna al sistema, necessaria al corretto funzionamento dello stesso.

Si noti, infine, che per la semantica di <<include>> ogni volta che viene inserito un nuovo evento sanitario nel sistema (avente determinate caratteristiche che ne rendono necessaria la sua notifica al medico), viene inviata al MMG/PLS la sua notifica.

Extension Points

I punti di estensione, che definiscono le condizioni da rispettare per l'invocazione degli Use Case "extended", sono:

- l'evento sanitario corrisponde alla creazione/sostituzione di un referto
- l'evento sanitario corrisponde alla creazione/aggiornamento di una prescrizione

[18] Ciò permette il popolamento del Fascicolo Sanitario Elettronico.

8.9.3 Use Case Notifica Nuovo Evento Sanitario

Descrizione

Il servizio notifica al MMG/PLS l'inserimento di un nuovo evento sanitario nel sistema. La notifica deve permettere al medico di discriminare immediatamente tra eventi sanitari di interesse o meno. Dovrà contenere (almeno) i seguenti campi:

- nome, cognome, data di nascita dell'assistito
- un riferimento che permette di recuperare le informazioni sull'evento sanitario tramite invocazione del servizio opportuno
- un elemento di identificazione dell'evento sanitario (es tipo dell'evento, data)
- l'indicazione del medico o della struttura che ha gestito l'evento

Attori

1. MMG/PLS

PreCondizioni

Il MMG/PLS è autenticato sul sistema ed è stato inserito un nuovo evento sanitario relativo ad un assistito del medico.

PostCondizioni

Il MMG/PLS riceve la notifica sulla creazione del nuovo evento sanitario riguardante il suo assistito.

Note implementative

Il meccanismo di notifica può essere basato sulla tecnica di Publish&Subscribe: il MMG/PLS sottoscrive la ricezione di determinati eventi sanitari riguardanti i suoi assistiti e automaticamente riceve la notifica.

8.10 Use Case Package Servizi Refertazione

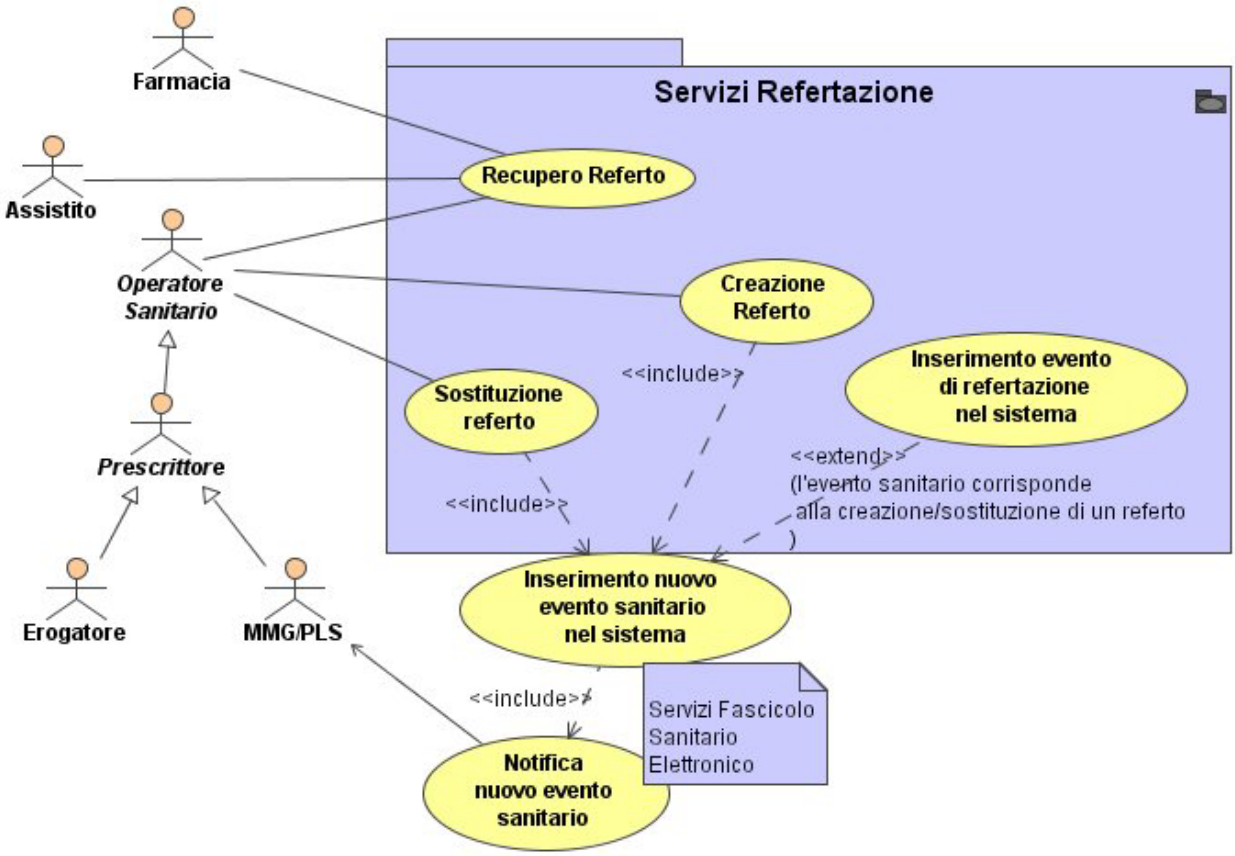


Figura 16. Servizi Refertazione

Fornisce servizi per la gestione dei referti. Per completezza sono riportati anche gli Use Case "Inserimento nuovo evento sanitario nel sistema" e "Notifica Nuovo Evento Sanitario", nonché

l'associazione tra MMG/PLS e quest'ultimo Use Case, appartenenti allo Use Case Package Servizi Fascicolo Sanitario Elettronico.

Relazioni interne
Association [Farmacia – Recupero Referto]
Association [Assistito - Recupero Referto]
Association [Operatore Sanitario – Recupero Referto]
Association [Operatore Sanitario - Creazione Referto]
Association [Operatore Sanitario - Sostituzione Referto]
Include [Creazione Referto – Servizi Fascicolo Sanitario Elettronico::Inserimento nuovo evento sanitario nel sistema]
Include [Sostituzione referto - Servizi Fascicolo Sanitario Elettronico::Inserimento nuovo evento sanitario nel sistema]
Extend [Inserimento evento di refertazione nel sistema - Servizi Fascicolo Sanitario Elettronico::Inserimento nuovo evento sanitario nel sistema]

8.10.1 Use Case Inserimento Evento di Refertazione nel Sistema

Descrizione

Scopo di questo servizio è l'inserimento, nel sistema, di eventi sanitari relativi alla creazione/sostituzione di referti. Tale Use Case estende lo Use Case Inserimento nuovo evento sanitario quando la condizione dell'extension point "l'evento sanitario corrisponde alla creazione/sostituzione di un referto" è verificata. Ogni evento di refertazione inserito del sistema deve essere associato al codice univoco del referto, in modo da poter essere recuperato tramite invocazione del servizio Recupero Referto.

Attori

Tutti gli attori degli Use Case Creazione Referto e Sostituzione referto.

PreCondizioni

Il nuovo evento sanitario registrato nel sistema è relativo alla creazione/sostituzione di un referto.

PostCondizioni

Il nuovo evento sanitario è registrato nel sistema.

8.10.2 Use Case Creazione Referto

Descrizione

Scopo di questo servizio è di creare e memorizzare un referto nel repository referti. E' di sua competenza anche l'inserimento del/dei riferimenti al nuovo evento sanitario (in questo caso la creazione del referto) nel sistema e la creazione della notifica di avvenuta refertazione al MMG/PLS dell'assistito. In particolare, ogni volta che un operatore sanitario crea un nuovo referto, viene anche:

- inserito un nuovo evento sanitario nel sistema, per la semantica di <<include>>; inoltre, poiché la condizione indicata dall'extension point è verificata (l'evento sanitario corrisponde alla creazione/sostituzione di un referto) viene invocato lo Use Case "extended" Inserimento evento di refertazione nel sistema.
- Notificato il nuovo evento sanitario al MMG/PLS, per la semantica di <<include>>.

Si noti che nel secondo caso si è ipotizzato che la notifica al medico sulla presenza del nuovo evento sanitario sia identica (in termini di meccanismo, dati inviati, ecc.) per tutte le tipologie di evento

sanitario che si sta considerando. In alternativa, si possono differenziare le varie notifiche in base all'evento sanitario in modo simile a quanto fatto per l'inserimento degli eventi sanitari nel sistema.

Un referto può fare riferimento:

- ad un'unica prestazione
- a più prestazioni

Un referto può far riferimento a prestazioni contenute in più prescrizioni, oppure più referti possono far rifermento ad un'unica prescrizione. Perciò, tale servizio consente di registrare un referto:

- associandolo ad una prescrizione o ad un insieme di prescrizioni, nel caso queste siano state registrate nel sistema;
- nel caso in cui il referto non faccia riferimento ad alcuna prescrizione registrata nel sistema, il servizio applicativo permette di inviare ugualmente la notifica solo se è possibile identificare in modo univoco l'assistito.

Attori

1. *Operatore Sanitario*
   a. *Prescrittore*
      i. Erogatore
      ii. MMG/PLS

PreCondizioni

L'operatore sanitario è autenticato dal sistema e il referto è firmato.

PostCondizioni

Il referto è registrato sul repository.

8.10.3 Use Case Sostituzione Referto

Descrizione

Questo servizio permette ad un sistema che abbia in precedenza trasmesso un referto di sostituirlo. E' di sua competenza anche l'inserimento del/dei riferimenti al nuovo evento sanitario (in questo caso la creazione del referto) nel sistema. Rispetto alla semplice creazione del referto, dovrà essere memorizzato nel sistema sia il riferimento al referto da sostituire, sia quello al nuovo referto che andrà memorizzato nel repository referti. Il vecchio referto andrà recuperato, posto nello stato di modificato e collegato al referto che lo sostituisce. Infine, spetta a questo servizio la creazione della notifica di avvenuta refertazione al medico prescrittore o di base. Di conseguenza, ogni volta che un operatore sanitario crea un nuovo referto, viene anche:

- inserito un nuovo evento sanitario nel sistema, per la semantica di <<include>>; inoltre, poiché la condizione indicata dall'extension point è verificata (l'evento sanitario corrisponde alla creazione/sostituzione di un referto) viene invocato lo Use Case "extended" Inserimento evento di refertazione nel sistema.
- Notificato il nuovo evento sanitario al MMG/PLS, per la semantica di <<include>>.

Si noti che nel secondo caso si è ipotizzato che la notifica al medico sulla presenza del nuovo evento sanitario sia identica (in termini di meccanismo, dati inviati, ecc.) per tutte le tipologie di evento sanitario che si sta considerando. In alternativa, si possono differenziare le varie notifiche in base all'evento sanitario in modo simile a quanto fatto per l'inserimento degli eventi sanitari nel sistema.

Attori

1. *Operatore Sanitario*
   a. *Prescrittore*
      i. Erogatore
      ii. MMG/PLS

PreCondizioni

L'operatore sanitario è autenticato dal sistema, il referto è firmato, ed è individuato il referto da sostituire.

PostCondizioni

Il referto sul sistema viene sostituito dal nuovo referto.

8.10.4 Use Case Recupero Referto

Descrizione

Tale servizio permette agli operatori sanitari abilitati di accedere ad un referto, ed in particolare, di:

- identificare il referto
- leggere e visualizzarne il contenuto.

Tale servizio è richiamabile:

- a seguito di notifica
- a seguito di interrogazione

La ricerca di un referto può avvenire secondo una serie di parametri, tra cui il codice univoco del referto, il codice sanitario dell'assistito, il codice univoco della prescrizione elettronica. Si possono presentare vari casi:

- i criteri di ricerca permettono di identificare univocamente il referto: questo viene presentato direttamente al richiedente;
- i criteri di ricerca permettono di identificare più referti associati ad un dato assistito, verranno mostrate al richiedente le ricorrenze identificate: a questo punto il richiedente seleziona la ricorrenza corrispondente al referto cercato ed esso verrà prelevato dal repository e visualizzato;
- i criteri di ricerca non permettono di identificare univocamente l'assistito (di cui si desidera recuperare il referto), verranno mostrati al richiedente alcuni dati dell'assistito, ai fini della sua univoca individuazione;
- i criteri di ricerca individuano più referti di più assistiti si procede inizialmente alla identificazione dell'assistito e in seguito a quella del referto.

Infine, può essere opportuno prevedere politiche per la gestione del consenso sulla visualizzazione del referto.

Si noti che il referto verrà memorizzato all'interno del Repository dell'azienda refertante che ha prodotto il referto, mentre il controllo del consenso andrà realizzato sull'azienda di assistenza (cui appartiene il paziente oggetto del referto). In generale, l'azienda di assistenza e l'azienda refertante saranno diverse, pertanto risulta necessaria una comunicazione tra le porte applicative aziendali (cfr. specifiche CNIPA – SPCC), che permetta di invocare i servizi applicativi e di effettuare i controlli necessari all'interno di aziende diverse da quella refertante.

Attori

1. Assistito
2. *Operatore Sanitario*
    a. *Prescrittore*
        i. Erogatore
        ii. MMG/PLS

3. Farmacia

PreCondizioni

L'attore viene identificato dal sistema e il referto da recuperare è stato registrato nel sistema.

PostCondizioni

L'attore recupera il referto cercato.

8.11 Use Case Package Servizi Prescrizione

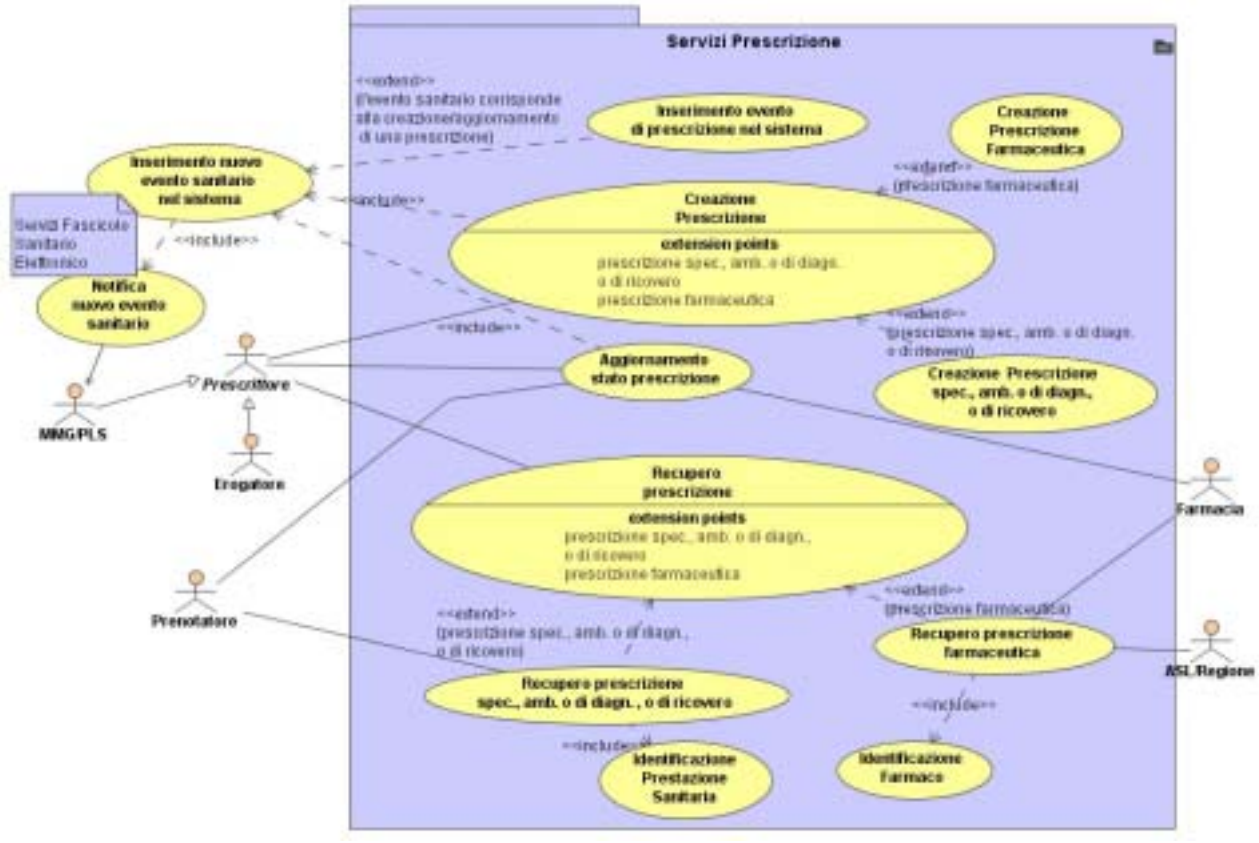


Figura 17. Servizi di prescrizione

Fornisce servizi per la gestione delle prescrizioni dell'assistito. Per completezza sono riportati gli Use Case "Inserimento nuovo evento sanitario nel sistema" e "Notifica Nuovo Evento Sanitario", nonché l'associazione tra MMG/PLS e quest'ultimo Use Case, appartenenti allo Use Case Package Servizi Fascicolo Sanitario Elettronico.

Relazioni interne
Association [Prescrittore - Creazione Prescrizione]
Association [Prescrittore – Aggiornamento stato prescrizione]
Association [Prescrittore - Recupero prescrizione]
Association [Prenotatore - Aggiornamento stato prescrizione]
Association [Prenotatore - Recupero prescrizione spec., amb. o di diagn., o di ricovero]
Association [Farmacia - Aggiornamento stato prescrizione]
Association [Farmacia - Recupero prescrizione farmaceutica]
Association [ASL/Regione - Recupero prescrizione farmaceutica]
Include [Creazione Prescrizione – Servizi Fascicolo Sanitario Elettronico::Inserimento nuovo evento sanitario nel sistema]
Include [Aggiornamento stato prescrizione - Servizi Fascicolo Sanitario Elettronico::Inserimento nuovo evento sanitario nel sistema]
Include [Recupero prescrizione spec., amb. o di diagn., o di ricovero - Identificazione Prestazione Sanitaria]

⎯Include [Recupero prescrizione farmaceutica - Identificazione Farmaco]
⎯Extend [Inserimento evento di prescrizione nel sistema - Servizi Fascicolo Sanitario Elettronico::Inserimento nuovo evento sanitario nel sistema]
⎯Extend [Creazione prescrizione spec., amb. o di diagn., o di ricovero – Creazione prescrizione]
⎯Extend [Creazione prescrizione farmaceutica - Creazione prescrizione]
⎯Extend [Recupero prescrizione spec., amb. o di diagn., o di ricovero - Recupero prescrizione]
⎯Extend [Recupero prescrizione farmaceutica - Recupero prescrizione]

8.11.1 Use Case Inserimento Evento di Prescrizione nel Sistema

Descrizione

Scopo di questo servizio è l'inserimento, nel sistema, di eventi sanitari relativi alla creazione di prescrizioni. Tale Use Case estende lo Use Case Inserimento nuovo evento sanitario quando la condizione dell'extension point "l'evento sanitario corrisponde alla creazione/aggiornamento di una prescrizione" è verificata. Ogni evento di prescrizione inserito del sistema deve essere associato al codice univoco che identifica la prescrizione (v. dopo), in modo da poter essere recuperato tramite invocazione del servizio Recupero Prescrizione.

Attori

Tutti gli attori degli Use Case Creazione Prescrizione e Aggiornamento stato prescrizione.

PreCondizioni

Il nuovo evento sanitario registrato nel sistema è relativo alla creazione/aggiornamento di una prescrizione.

PostCondizioni

Il nuovo evento sanitario è registrato nel sistema.

8.11.2 Use Case Creazione Prescrizione

Descrizione

Il servizio si occupa di gestire le prescrizioni elettroniche create dal prescrittore e di memorizzarle nel repository opportuno. Vengono considerate sia le prescrizioni farmaceutiche, sia quelle di diagnostica o di specialistica ambulatoriale. Poiché le modalità di memorizzazione possono dipendere dal tipo di prescrizione, sono stati definiti Use Case che estendono lo Use Case Creazione Prescrizione (Use Case Creazione Prescrizione Farmaceutica e Use Case Creazione Prescrizione di Specialistica, Ambulatoriale o di Diagnostica, o di Ricovero).

E' responsabilità del servizio:

- L'acquisizione e la trasmissione dei dati della prescrizione elettronica al sistema
- La memorizzazione di tali dati nell'istanza della prescrizione elettronica e attivare le opportune azioni di verifica della correttezza e invio di notifiche.

E' competenza del servizio anche l'inserimento del/dei riferimenti al nuovo evento sanitario (in questo caso la creazione della prescrizione) nel sistema e la creazione della notifica di avvenuta prescrizione al MMG/PLS dell'assistito. In particolare, ogni volta che un prescrittore crea una nuova prescrizione, viene anche:

- inserito un nuovo evento sanitario nel sistema, per la semantica di <<include>>; inoltre, poiché la condizione indicata dall'extension point è verificata (l'evento sanitario corrisponde alla creazione/aggiornamento di una prescrizione) viene invocato lo Use Case "extended" Inserimento evento di prescrizione nel sistema.

- notificato il nuovo evento sanitario al MMG/PLS, per la semantica di <<include>>.

Si noti che nel secondo caso si è ipotizzato che la notifica al MMG/PLS relativa alla presenza del nuovo evento sanitario sia identica (in termini di meccanismo, dati inviati, ecc.) per tutte le tipologie di evento sanitario che si sta considerando. In alternativa, si possono differenziare le varie notifiche in base all'evento sanitario in modo simile a quanto fatto per l'inserimento degli eventi sanitari nel sistema.

Extension Points

In base alla discussione precedente, i punti di estensione, che definiscono le condizioni da rispettare per l'invocazione degli Use Case "extended", distinguono tra:

- prescrizione farmaceutica
- prescrizione specialistica, ambulatoriale o di diagnostica, o di ricovero

Attori

1. *Prescrittore*
    a. Erogatore
    b. MMG/PLS

PreCondizioni

L'attore è identificato dal sistema.

PostCondizioni

Viene creata una nuova prescrizione e registrata nel repository opportuno.

Note implementative

Il servizio è accessibile tramite l'applicativo di cartella clinica dei medici, che deve essere integrato in modo da:

- generare il codice univoco della prescrizione;
- gestire il consenso.

8.11.3 Use Case Creazione prescrizione farmaceutica

Descrizione

Questo servizio gestisce le prescrizioni farmaceutiche create dal prescrittore e le memorizza nel repository opportuno: tale Use Case estende lo Use Case Creazione Prescrizione quando è verificata la condizione dell'extension point "prescrizione farmaceutica".

Attori

Tutti e soli gli attori dello Use Case Creazione Prescrizione

PreCondizioni

Quelle dello Use Case Creazione Prescrizione, con l'ulteriore vincolo che si crea una prescrizione farmaceutica.

PostCondizioni

Quelle dello Use Case Creazione Prescrizione.

8.11.4 Use Case Creazione prescrizione specialistica, ambulatoriale o di diagnostica, o di ricovero

Descrizione

Questo servizio gestisce sia le prescrizioni specialistiche, ambulatoriali o di diagnostica, sia le prescrizioni di ricovero create dal prescrittore e le memorizza nel repository opportuno: tale Use Case estende lo Use Case Creazione Prescrizione quando è verificata la condizione dell'extension point "prescrizione specialistica, ambulatoriale o di diagnostica, o di ricovero".

Attori

Tutti e soli gli attori dello Use Case Creazione Prescrizione.

PreCondizioni

Quelle dello Use Case Creazione Prescrizione, con l'ulteriore vincolo che si crea una prescrizione specialistica, ambulatoriale o di diagnostica, oppure una prescrizione di ricovero.

PostCondizioni

Quelle dello Use Case Creazione Prescrizione.

8.11.5 Use Case Aggiornamento stato prescrizione

Descrizione

Il servizio consente di aggiornare lo stato di una prescrizione. In linea generale, l'evolversi dello stato di una prescrizione è causato dagli attori, tuttavia si possono anche prevedere casi in cui esso sia sotto il controllo del sistema (a seguito di controlli eseguiti). Il servizio può inoltre essere invocato dal sistema in seguito alla creazione di un referto o di un ricovero per aggiornare lo stato della prescrizione (in refertata o in ricovero).

E' responsabilità del servizio la modifica degli stati di: Ricovero, Annullata, Prenotata, Accettata e Refertata di una prescrizione.

Per ciascun attore è necessario definire quali stati può modificare e quali modifiche può apportare.

E' competenza del servizio anche l'inserimento del/dei riferimenti al nuovo evento sanitario (in questo caso l'aggiornamento dello stato della prescrizione) nel sistema e la creazione della notifica di aggiornamento al MMG/PLS dell'assistito. In particolare, ogni volta che lo stato di una prescrizione è aggiornato, viene anche:

- inserito un nuovo evento sanitario nel sistema, per la semantica di <<include>>; inoltre, poiché la condizione indicata dall'extension point è verificata (l'evento sanitario corrisponde alla creazione/aggiornamento di una prescrizione) viene invocato lo Use Case "extended" Inserimento evento di prescrizione nel sistema.
- notificato il nuovo evento sanitario al MMG/PLS, per la semantica di <<include>>.

Si noti che nel secondo caso si è ipotizzato che la notifica al MMG/PLS relativa alla presenza del nuovo evento sanitario sia identica (in termini di meccanismo, dati inviati, ecc.) per tutte le tipologie di evento sanitario che si sta considerando. In alternativa, si possono differenziare le varie notifiche in base all'evento sanitario in modo simile a quanto fatto per l'inserimento degli eventi sanitari nel sistema.

Attori

1. *Prescrittore*
   a. Erogatore
   b. MMG/PLS
2. Prenotatore
3. Farmacia

PreCondizioni

L'attore è autenticato sul sistema e la prescrizione cercata è memorizzata nel sistema.

PostCondizioni

Lo stato della prescrizione è aggiornato.

8.11.6 Use Case Recupero prescrizione

Descrizione

Il servizio si occupa di recuperare dal sistema i dati di una prescrizione emessa dal prescrittore, restituendo anche l'informazione relativa allo stato in cui si trova la prescrizione (annullata, prenotata, accettata, refertata,...). Vengono considerate sia le prescrizioni farmaceutiche, sia quelle specialistiche, ambulatoriali o di diagnostica, oppure quelle di ricovero. Poiché le modalità di memorizzazione possono dipendere dal tipo di prescrizione, sono stati definiti Use Case che estendono lo Use Case Recupero Prescrizione (Use Case Recupero Prescrizione Farmaceutica e Use Case Recupero Prescrizione Ambulatoriale, di Diagnostica o di Specialistica, o di Ricovero).

Il servizio è responsabile di:

- Identificare la prescrizione all'interno del repository

- Identificare la prestazione associata alla prescrizione o il farmaco
- Presentare i dati recuperati secondo le modalità di visualizzazione previste.

Il servizio applicativo deve poter essere utilizzato dagli operatori sanitari che sono abilitati ad accedere alle informazioni presenti sulle prescrizioni.

L'interrogazione per il recupero della prescrizione può avvenire inserendo alcuni tra i seguenti campi:

- Codice univoco prescrizione
- Codice Fiscale
- Codice Sanitario
- Data di emissione della prescrizione
- Codice Azienda
- ...

Nel caso in cui tra i campi inseriti per la ricerca sia presente il codice della prescrizione, sarà possibile individuare in modo univoco la prescrizione e quindi viene presentata all'attore direttamente la prescrizione recuperata.

Extension Points

In base alla discussione precedente, i punti di estensione, che definiscono le condizioni da rispettare per l'invocazione degli Use Case "extended", distinguono tra:

- prescrizione farmaceutica
- prescrizione specialistica, ambulatoriale o di diagnostica, o di ricovero.

Attori

1. *Prescrittore*
    a. Erogatore
    b. MMG/PLS

PreCondizioni

L'attore è autenticato dal sistema e la prescrizione cercata esiste nel sistema.

PostCondizioni

L'attore recupera la prescrizione cercata.

8.11.7 Use Case Recupero prescrizione farmaceutica

Descrizione

Questo servizio permette di recuperare dal sistema i dati di una prescrizione farmaceutica emessa dal prescrittore, restituendo anche l'informazione relativa allo stato in cui si trova la prescrizione. Tale Use Case estende lo Use Case Recupero Prescrizione quando è verificata la condizione dell'extension point "prescrizione farmaceutica". In più, offre la funzionalità di identificazione del farmaco contenuto alla prescrizione farmaceutica che è stata recuperata. Ciò è indicato mediante la relazione <<include>> tra il presente Use Case e lo Use Case Identificazione Farmaco.

Attori

Tutti gli attori dello Use Case Recupero prescrizione, ed in aggiunta:

1. Farmacia
2. ASL/Regione.

PreCondizioni

Quelle dello Use Case Recupero prescrizione, con l'ulteriore vincolo che si cerca una prescrizione farmaceutica.

PostCondizioni

Quelle dello Use Case Recupero prescrizione.

8.11.8 Use Case Recupero prescrizione specialistica, ambulatoriale o di diagnostica, o di ricovero

Descrizione

Questo servizio permette di recuperare dal sistema i dati di una prescrizione specialistica, ambulatoriale o di diagnostica, oppure di una prescrizione di ricovero emessa dal prescrittore, restituendo anche l'informazione relativa allo stato in cui si trova la prescrizione. Tale Use Case estende lo Use Case Recupero Prescrizione quando è verificata la condizione dell'extension point "prescrizione specialistica, ambulatoriale o di diagnostica, o di ricovero". In più, offre la funzionalità di identificazione della prestazione sanitaria associata alla prescrizione che è stata recuperata. Ciò è indicato mediante la relazione <<include>> tra il presente Use Case e lo Use Case Identificazione Prestazione Sanitaria.

Attori

Tutti gli attori dello Use Case Recupero prescrizione, ed in aggiunta:

1. Prenotatore.

PreCondizioni

Quelle dello Use Case Recupero prescrizione, con l'ulteriore vincolo che si cerca una prescrizione specialistica, ambulatoriale o di diagnostica, o una prescrizione di ricovero.

PostCondizioni

Quelle dello Use Case Recupero prescrizione.

8.11.9 Use Case Identificazione Prestazione Sanitaria

Descrizione

Il servizio permette di individuare il codice della prestazione cui la prescrizione recuperata si riferisce.

Attori

Tutti e soli gli attori dello Use Case Recupero prescrizione specialistica, ambulatoriale o di diagnostica, o di ricovero.

PreCondizioni

L'operatore sanitario è identificato dal sistema e ha recuperato la prescrizione cercata.

PostCondizioni

L'operatore sanitario ha identificato il codice della prestazione associata alla prescrizione recuperata.

8.11.10 Use Case Identificazione Farmaco

Descrizione

Il servizio permette di individuare il codice del farmaco contenuto nella prescrizione farmaceutica recuperata.

Attori

Tutti e soli gli attori dello Use Case Recupero prescrizione farmaceutica.

PreCondizioni

L'attore è identificato dal sistema e ha recuperato la prescrizione farmaceutica cercata.

PostCondizioni

L'attore ha identificato il codice del farmaco.

8.12 Use Case Package Scheda Sanitaria Individuale del Paziente

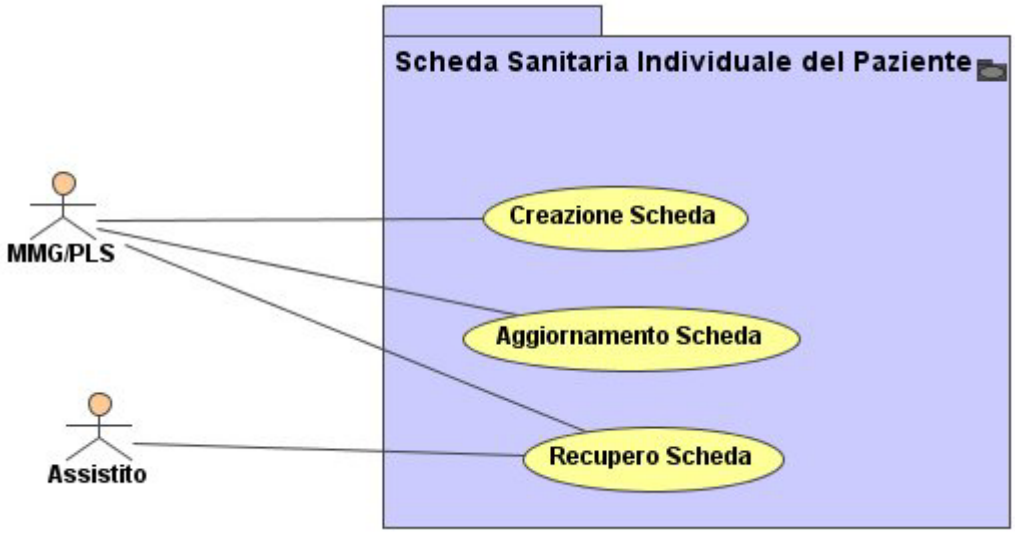


Figura 18. Scheda Sanitaria Individuale del Paziente

Fornisce un servizio per la gestione della scheda sanitaria individuale dell'assistito, contenente un riassunto degli eventi clinici e della storia sanitaria che caratterizzano ciascun paziente, ed in particolare, la sua anamnesi. Essa è aggiornata a seguito di particolari eventi sanitari che modificano in modo sostanziale la storia clinica del paziente.

Relazioni Interne
Association [MMG/PLS – Creazione Scheda]
Association [MMG/PLS – Aggiornamento Scheda]
Association [MMG/PLS – Recupero Scheda]
Association [Assistito – Recupero Scheda]

8.12.1 Use Case Creazione Scheda

Descrizione

Questo servizio crea una nuova scheda relativa ad un nuovo assistito, inserendone i dati statici, come:

- dati anagrafici
- anamnesi (ossia tutti i dati riguardanti i precedenti fisiologici e patologici, personali ed ereditari, dell'assistito)

Attori

1. MMG/PLS

PreCondizioni

Il MMG/PLS è autenticato sul sistema

PostCondizioni

Nel repository opportuno viene memorizzata la scheda sanitaria individuale del paziente, contenente dati "statici"

Note implementative

In generale, i MMG/PLS possono operare solo sui propri assistiti. Possono operare su altri pazienti solo in base ad una specifica autorizzazione.

8.12.2 Use Case Aggiornamento Scheda

Descrizione

Questo servizio permette l'aggiornamento della scheda sanitaria individuale dell'assistito in presenza di determinati eventi sanitari che il MMG/PLS stabilirà opportunamente. Si può ipotizzare che in taluni casi tale aggiornamento avvenga automaticamente ogni volta che gli eventi sanitari individuati vengono aggiunti al sistema.

Attori

1. MMG/PLS

PreCondizioni

Il MMG/PLS è autenticato dal sistema; la scheda sanitaria individuale dell'assistito è stata registrata nel sistema; e il MMG/PLS ha ricevuto notifica di un evento sanitario relativo all'assistito, che ritiene necessario inserire nella sua scheda individuale.

PostCondizioni

La scheda sanitaria individuale dell'assistito è aggiornata con nuovi dati.

Note implementative

In generale, i MMG/PLS possono operare solo sui propri assistiti. Possono operare su altri pazienti solo in base ad una specifica autorizzazione.

8.12.3 Use Case Recupero Scheda

Descrizione

Questo servizio permette l'accesso in lettura (per la visualizzazione a schermo, la stampa, ecc.) della Scheda Sanitaria Individuale. Poiché essa non viene modificata, anche l'assistito può utilizzare questo servizio.

Attori

1. MMG/PLS
2. Assistito

PreCondizioni

L'attore è autenticato dal sistema e la scheda sanitaria individuale dell'assistito è stata registrata nel sistema.

PostCondizioni

L'attore recupera la scheda cercata.

Note implementative

In generale, i MMG/PLS possono operare solo sui propri assistiti. Possono operare su altri pazienti solo in base ad una specifica autorizzazione.