Regione Campania

Il Commissario ad Acta per l'attuazione
del Piano di rientro dai disavanzi del SSR Campano
(Deliberazione Consiglio dei Ministri 10/07/2017)

DECRETO N. 34 DEL 29.03.2019

OGGETTO: Approvazione linee di indirizzo per l'implementazione del sistema informativo sanitario regionale

(Deliberazione del Consiglio dei Ministri 10/07/2017 punto vii: "attuazione degli interventi rivolti all'incremento della produttività e della qualità dell'assistenza erogata dagli Enti del Servizio sanitario regionale")

VISTA la legge 30 dicembre 2004, n. 311 recante " Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2005) e, in particolare, l'art. 1, comma 180, che ha previsto per le regioni interessate l'obbligo di procedere, in presenza di situazioni di squilibrio economico finanziario, ad una ricognizione delle cause ed alla conseguente elaborazione di un programma operativo di riorganizzazione, di riqualificazione o di potenziamento del Servizio sanitario regionale, di durata non superiore ad un triennio;

VISTA l'Intesa Stato-Regioni del 23 marzo 2005 che, in attuazione della richiamata normativa, pone a carico delle Regioni l'obbligo di garantire, coerentemente con gli obiettivi di indebitamento netto delle amministrazioni pubbliche, l'equilibrio economico-finanziario del servizio sanitario regionale nel suo complesso, realizzando forme di verifica trimestrale della coerenza degli andamenti con gli obiettivi assegnati in sede di bilancio preventivo per l'anno di riferimento, nonché la stipula di un apposito accordo che individui gli interventi necessari per il perseguimento dell'equilibrio economico, nel rispetto dei livelli essenziali di assistenza;

VISTA la delibera della Giunta regionale della Campania n. 460 del 20/03/2007 - *"Approvazione del Piano di Rientro dal disavanzo e di riqualificazione e razionalizzazione del Servizio sanitario Regionale ai fini della sottoscrizione dell'Accordo tra Stato e Regione Campania ai sensi dell'art. 1, comma 180, della legge n. 311/2004";*

VISTA la delibera del Consiglio dei Ministri in data 24 luglio 2009 con il quale il Governo ha proceduto alla nomina del Presidente pro tempore della Regione Campania quale Commissario ad Acta per l'attuazione del piano di rientro dal disavanzo sanitario ai sensi dell'art. 4, comma 2, del DL 1 ottobre 2007, n. 159, convertito con modificazioni dalla L. 29 novembre 2007, n. 222;

VISTA la delibera del Consiglio dei Ministri dell'11 dicembre 2015, con la quale sono stati nominati quale Commissario ad Acta il dott. Joseph Polimeni e quale Sub Commissario ad acta il Dott. Claudio D'Amario;

VISTA la delibera del Consiglio dei Ministri del 10 Luglio 2017 con la quale, all'esito delle dimissioni del dott. Polimeni dall'incarico commissariale, il Presidente della Giunta Regionale è stato nominato Commissario ad Acta per l'attuazione del vigente piano di rientro dal disavanzo del SSR Campano, secondo i programmi operativi di cui all'articolo 2, comma 88, della legge 23 dicembre 2009, n. 191 e *ss.mm.ii.*;

VISTA la richiamata deliberazione del 10 luglio 2017 che:

Regione Campania

Il Commissario ad Acta per l'attuazione
del Piano di rientro dai disavanzi del SSR Campano
(Deliberazione Consiglio dei Ministri 10/07/2017)

- assegna al Commissario ad acta l'incarico prioritario di attuare i Programmi operativi 2016-2018 e gli interventi necessari a garantire, in maniera uniforme sul territorio regionale, l'erogazione dei livelli essenziali di assistenza in condizioni di efficienza, appropriatezza, sicurezza e qualità, nei termini indicati dai Tavoli tecnici di verifica, nell'ambito della cornice normativa vigente;

- individua, nell'ambito del più generale mandato sopra specificato, alcune azioni ed interventi come acta ai quali dare corso prioritariamente e, segnatamente, al punto vii *"attuazione degli interventi rivolti all'incremento della produttività e della qualità dell'assistenza erogata dagli Enti del Servizio sanitario regionale";*

VISTA la comunicazione, assunta al protocollo della Struttura Commissariale n. 430 del 9 Febbraio 2018, con la quale il Sub Commissario Dott. Claudio D'Amario ha rassegnato le proprie dimissioni per assumere la funzione di Direttore Generale della Prevenzione Sanitaria presso il Ministero della Salute;

RICHIAMATA la sentenza del Consiglio di Stato n. 2470/2013, secondo cui *"nell'esercizio dei propri poteri, il Commissario ad acta agisce quale "organo decentrato dello Stato ai sensi dell'art. 120 della Costituzione, che di lui si avvale nell'espletamento di funzioni d'emergenza stabilite dalla legge, in sostituzione delle normali competenze regionali", emanando provvedimenti qualificabili come "ordinanze emergenziali statali in deroga", ossia "misure straordinarie che il commissario, nella sua competenza d'organo statale, è tenuto ad assumere in esecuzione del piano di rientro, così come egli può emanare gli ulteriori provvedimenti normativi, amministrativi, organizzativi e gestionali necessari alla completa attuazione del piano di rientro*";

PREMESSO che

- Il ruolo dell' *Information Technology* in ambito sanitario è diventato ormai centrale, vero punto di riferimento per il governo e per il monitoraggio dell'attività socio-sanitaria e amministrativa delle Aziende Sanitarie Locali e Ospedaliere;

- i livelli di progettazione dei sistemi informativi, di pianificazione degli investimenti e di monitoraggio dei risultati raggiunti trovano la loro dimensione ottimale nel livello regionale, scala di riferimento più opportuna per la valutazione globale dei progetti;

- anche le normative nazionali fanno ampio riferimento all'utilizzo dei sistemi informativi il miglioramento dei livelli di servizio in ambito sanitario;

- l'art. 17 della legge 98/2013 ("Conversione, con modificazioni, del decreto legge 21 giugno 2013, n. 69 Disposizioni urgenti per il rilancio dell'economia"), riprendendo l'art.12 del decreto legge 18 ottobre 2012 n. 179 convertito con modificazioni dalla legge 17 dicembre 2012 n. 221, ha stabilito che la realizzazione del Fascicolo Sanitario Elettronico rientra tra gli adempimenti a cui sono tenute le regioni e le province autonome per l'accesso al finanziamento integrativo a carico del Servizio Sanitario Nazionale;

CONSIDERATO che

- l'innovazione digitale dei processi sanitari è un passaggio fondamentale per migliorare il rapporto costo-qualità dei servizi, limitare sprechi e inefficienze, ridurre le differenze tra i

territori, nonché innovare le relazioni di front-end per migliorare la qualità percepita dal cittadino;

- le attività devono svilupparsi lungo le linee d'intervento previste dal "Patto della salute" del Ministero della Salute, quali passaggi fondamentali e prioritari per costruire il futuro della sanità digitale. Si tratta, infatti, di sviluppo di soluzioni completamente integrate, caratterizzate da una forte interazione dei sistemi informativi sanitari, aziendali e ospedalieri, basate sull'utilizzo diffuso di tecnologie Cloud e sulla rigorosa applicazione di criteri per l'omogeneizzazione e la standardizzazione dei dati sanitari;

- l'integrazione dei dati è il presupposto per favorire la corretta interazione di tutti gli attori interessati. Su queste linee d'intervento, e con l'obiettivo primario di garantire la continuità assistenziale, si potranno consolidare sistemi informativi territoriali su cui impiantare modelli organizzativi innovativi, in grado di erogare servizi ad assistiti e operatori anche a supporto delle attività socio-sanitarie territoriali, per agevolare la diagnostica e sostenere i percorsi di cura e gestione delle cronicità;.

- il modello stesso di SSN, che trova nei sistemi regionali le declinazioni territoriali, deve essere la garanzia di accesso uniforme per il cittadino alle informazioni di tipo clinico/assistenziale a livello regionale. Esigenza comune anche agli operatori del SSR che devono poter accedere alle informazioni dei pazienti in modo sistematico e omogeneo, nel rispetto dei livelli di sicurezza e delle norme sulla privacy stabiliti dal regolamento europeo adottato il 25 maggio 2018, indipendentemente dall'ambito del sistema aziendale di registrazione dei dati;

RILEVATO che gli uffici della Direzione Generale Tutela della Salute hanno redatto all'esito della competente istruttoria il documento "Linee di indirizzo per l'implementazione del sistema informativo regionale" concernente:

1. la razionalizzazione dell'infrastruttura dei data center delle Aziende Sanitarie e la migrazione verso il cloud;
2. la connettività;
3. le prescrizioni e i principi per lo sviluppo, la manutenzione, l'evoluzione e la conduzione di sistemi informativi delle Aziende Sanitarie;

RAVVISATA la necessità di provvedere all'adozione delle indicate linee di indirizzo per la progettazione, lo sviluppo e la gestione dei Sistemi informativi delle Aziende Sanitarie Campane;

VISTI

- il D.L. 18 ottobre 2012, n. 179, recante "Ulteriori misure urgenti per la crescita del Paese" (convertito, con modificazioni, dalla L. 17 dicembre 2012, n. 221), ha istituito il Fascicolo Sanitario Elettronico (FSE);
- il D.L. 21 giugno 2013, n. 69, recante "Disposizioni urgenti per il rilancio dell'economia" (convertito, con modificazioni, dalla L. 9 agosto 2013, n.98) di modifica al D.L. n. 179/2012;
- il DPCM n.178 del 29 settembre 2015, pubblicato sulla G.U. dell'11 novembre 2015, n. 263, che ha emanato il "Regolamento in materia di fascicolo sanitario elettronico.";

Regione Campania

Il Commissario ad Acta per l'attuazione
del Piano di rientro dai disavanzi del SSR Campano
(Deliberazione Consiglio dei Ministri 10/07/2017)

- il DPCM n.14 novembre 2015, pubblicato sulla Gazzetta ufficiale n.303 del 31 dicembre 2015, che definisce le "modalità di attuazione del comma 2 dell'articolo 13 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modifiche, dalla legge 17 dicembre 2012, n. 221, in materia di prescrizioni farmaceutiche in formato digitale", in vigore dal 1° gennaio 2016";
- il DM 9 Dicembre 2015 recante le "Condizioni di erogabilità e indicazioni di appropriatezza prescrittiva delle prestazioni di assistenza ambulatoriale erogabili nell'ambito del Servizio sanitario nazionale", pubblicato sulla Gazzetta ufficiale n.15 del 20 gennaio 2016;
- il Piano Triennale per l'Informatica nella Pubblica amministrazione 2017 – 2019 approvato il 31/05/2017 dal Presidente del Consiglio dei Ministri e realizzato da AgID e dal Team per la Trasformazione Digitale;
- le Linee guida per la presentazione dei piani di progetto regionali per il FSE;
- la Delibera di Giunta Regionale n. 559 del 17/9/2017;
- la Delibera di Giunta Regionale n. 25 del 18/01/2018;
- il Decreto commissariale n. 26 del 22/2/2019;

Alla stregua dell'istruttoria tecnico-amministrativa effettuata dalla Direzione Generale per la Tutela della Salute e il Coordinamento del SSR

DECRETA

per tutto quanto esposto in premessa e che qui si intende integralmente riportato

di **APPROVARE** le *"Linee di indirizzo per l'implementazione del Sistema Informativo Sanitario Regionale"* che allegate al presente provvedimento ne formano parte integrante e sostanziale;

di **STABILIRE** che le Aziende sanitarie campane nella progettazione, implementazione, gestione e conduzione dei sistemi informativi devono applicare i principi contenuti nelle citate linee di indirizzo ed assicurare che tutte le attività connesse siano espletate in piena coerenza con le stesse;

di **TRASMETTERE** il presente provvedimento ai Ministeri affiancanti, riservandosi di adeguarlo alle eventuali osservazioni formulate dagli stessi;

di **INVIARE** il presente provvedimento all'Ufficio di Gabinetto del Presidente della Giunta regionale, all'Assessore regionale al Bilancio e al finanziamento del servizio sanitario regionale in raccordo con il Commissario ad acta per il piano di rientro dal disavanzo sanitario, alla Direzione Generale per la Tutela della Salute ed il Coordinamento del S.S.R., alle Aziende Sanitarie della Campania, al BURC per tutti gli adempimenti in materia di pubblicità e trasparenza.

Il Direttore Generale
per la Tutela della Salute
e il Coordinamento del SSR
Avv. Antonio Postiglione

DE LUCA

REGIONE CAMPANIA – LINEE D'INDIRIZZO PER L'IMPLEMENTAZIONE DEL SISTEMA INFORMATIVO SANITARIO REGIONALE

Versione 1.0
Ottobre 2018

SOMMARIO

1. Premessa: La Sanità Digitale

Il ruolo dell'Information Technology in ambito sanitario è diventato ormai centrale, vero punto di riferimento per il governo e per il monitoraggio dell'attività socio-sanitaria e amministrativa delle Aziende Sanitarie Locali e Ospedaliere. È altrettanto inconfutabile che i livelli di progettazione dei sistemi informativi, di pianificazione degli investimenti e di monitoraggio dei risultati raggiunti trovano la loro dimensione ottimale nel livello regionale, scala di riferimento più opportuna per la valutazione globale dei progetti.

Anche le normative nazionali fanno ampio riferimento all'utilizzo dei sistemi informativi come fattore abilitante per migliorare i livelli di servizio in ambito sanitario.

A tal proposito occorre rilevare come, ad esempio, l'art. 17 della legge 98/2013 ("Conversione, con modificazioni, del decreto-legge 21 giugno 2013, n. 69 Disposizioni urgenti per il rilancio dell'economia"), riprendendo l'art.12 del decreto legge 18 ottobre 2012 n. 179 convertito con modificazioni dalla legge 17 dicembre 2012 n. 221, ha fatto sì che la realizzazione del Fascicolo Sanitario Elettronico fosse compresa tra gli adempimenti cui sono tenute le regioni e le province autonome per l'accesso al finanziamento integrativo a carico del Servizio Sanitario Nazionale da verificare da parte del Comitato di cui all'articolo 9 dell'Intesa sancita il 23 marzo 2005 dalla Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano (altresì noto come il Comitato di verifica dei Livelli Essenziali di Assistenza).

Al tempo stesso, nella medesima norma, all'art. 16 "Razionalizzazione dei CED Centri elaborazione dati", riprendendo l'art.33-septies del decreto-legge 18 ottobre 2012 n. 17, è promossa un'importante azione di consolidamento e razionalizzazione dei siti e delle infrastrutture digitali delle amministrazioni pubbliche (datacenter – apparati di calcolo e apparati di memorizzazione di massa – e rete – apparati per la connessione).

È chiaro, quindi, che i crescenti e sempre più importanti obiettivi in ambito ICT, derivanti sia dagli atti e dalle azioni regionali che dalle norme nazionali, richiedono di essere affrontate con un'economia di scala che non può più essere quella di ogni singola Azienda Sanitaria.

Il modello stesso di SSN, che trova nei sistemi regionali le opportune declinazioni territoriali, deve essere la garanzia per il cittadino di accesso uniforme alle proprie informazioni di tipo clinico/assistenziale a livello almeno regionale. Medesima esigenza è quella degli operatori del SSR, che devono poter accedere alle informazioni dei pazienti in modo sistematico e omogeneo, secondo i livelli di sicurezza e privacy definiti dall'entrata a regime del nuovo regolamento europeo a far data dal 25 maggio 2018, indipendentemente dai sistemi aziendali in cui i dati sono stati registrati.

Le azioni perseguite a livello regionale hanno visto, dapprima, una forte iniziativa in ambito di processi amministrativi attraverso il progetto SIAC per poi affrontare il processo di convergenza informativa anche nella gestione dei processi di prevenzione, diagnosi, cura e riabilitazione. Queste azioni non possono, però, prescindere dall'implementazione di modelli organizzativi efficaci e resilienti, che garantiscano un complessivo miglioramento della qualità del sistema attraverso l'impiego sistematico e sostenibile dell'innovazione tecnologica, con conseguente azzeramento dei costi non necessari.

2. Strategia per la crescita digitale 2014-2020 - Sanità Digitale a livello nazionale[1]

L'innovazione digitale dei processi sanitari è un passaggio fondamentale per migliorare il rapporto costo-qualità dei servizi sanitari, limitare sprechi e inefficienze, ridurre le differenze tra i territori, nonché innovare le relazioni di front-end per migliorare la qualità percepita dal cittadino.

Le attività si svilupperanno lungo le seguenti linee d'intervento nell'ambito del "Patto della salute" del Ministero della Salute, che rappresentano altrettanti passaggi fondamentali e prioritari per creare un contesto organico necessario a costruire il futuro della sanità digitale. Si tratta, infatti, di sviluppare soluzioni completamente integrate, caratterizzate da una forte interazione dei sistemi informativi sanitari, aziendali e ospedalieri, e basate sull'utilizzo diffuso di tecnologie Cloud, sull'applicazione di criteri per omogeneizzare e standardizzare la raccolta e il trattamento dei dati sanitari. L'integrazione è il presupposto per favorire una corretta interazione di tutti gli attori interessati. Su queste linee d'intervento, e con l'obiettivo primario di garantire la continuità assistenziale, si potranno consolidare sistemi informativi territoriali su cui impiantare modelli organizzativi innovativi, che siano in grado di erogare servizi ad assistiti e operatori anche a supporto delle attività socio-sanitarie territoriali, come agevolare la diagnostica, sostenere i percorsi di cura e gestire le cronicità.

Si potranno, finalmente, sviluppare e diffondere in modo capillare la telemedicina, il telemonitoraggio e il teleconsulto, che richiedono l'uso di strumenti elettromedicali innovativi, sensori, videocomunicazione e altri apparati, sia per controllo a distanza del paziente che per agevolare il colloquio tra questo e gli operatori sanitari. In un simile contesto tecnologico, ad alta affidabilità e sicurezza, sarà possibile effettuare ampie analisi degli esiti clinico-assistenziali, mediante attività di business intelligence di settore.

Le linee di intervento strategico:

- Fascicolo sanitario elettronico

Si intende procedere alla realizzazione del Fascicolo Sanitario Elettronico (FSE) del cittadino, inteso come l'insieme di documenti clinici (patient summary, referti, prescrizioni, ecc.) inerenti al proprio stato di salute e derivanti dal proprio rapporto con i diversi attori del Servizio Sanitario Nazionale.

- Ricette digitali

Occorre completare la sostituzione delle prescrizioni farmaceutiche e specialistiche cartacee con gli equivalenti documenti digitali. La Regione Campania è ai primi posti a livello nazionale per la dematerializzazione delle ricette farmaceutiche, adesso occorre costruire servizi per favorire i cittadini nell'utilizzo degli strumenti digitali.

- Dematerializzazione dei referti medici e delle cartelle cliniche

Per migliorare i servizi ai cittadini, riducendone i costi connessi, è necessario accelerare il processo di dematerializzazione dei referti medici e delle cartelle cliniche, rendendoli disponibili anche online.

- Prenotazioni online

[1] https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strat_crescita_digit_3marzo_0.pdf

Accelerare la diffusione dei Centri Unici di Prenotazione (sia online sia attraverso intermediari, es. farmacie) delle prestazioni sanitarie a livello regionale e sovra territoriale, al fine di ottimizzare l'impiego delle risorse e ridurre i tempi di attesa.

Per ogni linea d'intervento sono già state realizzate o sono in corso molte attività:

Fascicolo sanitario elettronico

- A livello nazionale: a) il Garante per la protezione dei dati personali ha emanato le "Linee guida in tema di FSE" il 16 luglio 2009; b) il Ministero della salute (con le Regioni, il Garante per la protezione dei dati personali e la PCM (ex Dipartimento per la digitalizzazione DDI, ora confluito nell'Agenzia per l'Italia digitale - AgID) ha elaborato le linee guida nazionali per l'istituzione del FSE, approvate il 10 febbraio 2011 dalla Conferenza Stato-Regioni; c) la PCM (ex DDI) e il CNR hanno elaborato, in accordo con Regioni, le Linee guida per l'interoperabilità del FSE a livello sovra regionale, nel contesto del sistema pubblico di connettività (SPC). d) la previsione normativa per l'istituzione del FSE è stata inserita nel DL 179/2012 DDL (articolo12), poi modificata e rafforzata con il DL 69/2013: 1) le regioni devono istituire il FSE entro il 30 giugno 2015, nel rispetto dei criteri definiti con apposito DPCM attuativo (in fase di emanazione), secondo un Piano di progetto presentato entro il 30 giugno 2014 (tutte le regioni hanno presentato il piano di progetto ad AgID nei tempi previsti), redatto sulla base di linee guida emanate da AgID (pubblicate il 30 marzo 2014) e approvato, entro il 30 agosto 2014, da apposito gruppo di lavoro istituito da AgID e il Ministero della salute (le attività di valutazione si sono completate ma si è in attesa dell'emanazione del DPCM attuativo); 2) al fine di favorire l'interoperabilità delle soluzioni di FSE sviluppate a livello regionale, anche accentrando funzionalità comuni a più soluzioni, è prevista la possibilità di creazione di apposita piattaforma tecnologica a cura di AgID.
- A livello regionale: tutte le regioni stanno investendo nello sviluppo di soluzioni di FSE.
- La legge di stabilità 2013 ha istituito l'Anagrafe nazionale degli assistiti (da realizzarsi, a cura del Ministero della salute e del MEF, sulla base dell'Anagrafe nazionale della popolazione residente) che rappresenta un importante elemento di semplificazione per la realizzazione di un'architettura federata del FSE

Ricette digitali

L'art. 50 della legge 24 novembre 2003, n.326 (modificato dalla legge finanziaria 2007) ha introdotto l'obbligo di trasmissione telematica dei dati delle ricette ai fini del controllo della spesa.

- Il D.L. 31 maggio 2010 n.78 (art 11, comma 16) ha dato valore legale alla trasmissione telematica dei dati delle ricette (scompare la "ricetta rossa" cartacea).
- Il decreto dirigenziale del Ministero dell'economia e delle finanze del 2 novembre 2011 disciplina le modalità tecniche per attuazione del D.L. 31 maggio 2010 n.78 (il medico compila la ricetta online senza rilasciare nessun documento "formale" al paziente, ma solo un "promemoria" che riporta il numero di identificazione della ricetta. Il paziente si reca in farmacia e ritira il medicinale mostrando la propria tessera sanitaria e il "promemoria") e

rimanda, per la definizione dei piani di adozione della nuova procedura, alla stipula di accordi con le regioni (entro settembre 2012).

- Il DL 179/2012 ha previsto un'accelerazione in tema d'introduzione delle ricette elettroniche inserendo l'obbligo per tutte le regioni di provvedere, entro giugno 2014 e sulla base di apposite convenzioni stipulate con il MEF, alla graduale sostituzione delle prescrizioni in formato cartaceo con le equivalenti in formato elettronico, in percentuali di almeno il 60%nel 2013, l'80% nel 2014, il 90% nel 2015. Inoltre, mediante apposito decreto attuativo, è prevista la validità a livello nazionale delle ricette farmaceutiche in formato elettronico (rimane validità al solo livello regionale per quelle prescritte in formato cartaceo).

Dematerializzazione dei referti medici e delle cartelle cliniche

- Il Garante per la protezione dei dati personali ha emanato le " Linee guida in tema di referti online" il 19 novembre 2009.
- Il D.L. 13 maggio 2011, n. 70, ha introdotto l'obbligo di refertazione online (e pagamenti elettronici) per tutte le aziende sanitarie (DPCM attuativo 8 agosto 2013);
- Il Ministero della salute ha emanato le "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini" mentre Federsanità-ANCI (in collaborazione con il Dipartimento per la digitalizzazione della Presidenza del Consiglio dei Ministri) ha pubblicato le linee guida per le aziende sanitarie per la refertazione online.
- Il DL 179/2012 ha rafforzato le previsioni dell'articolo 47-bis del D.L. 9 febbraio 2012, n.5, ("Semplifica Italia"), per consentire la conservazione delle cartelle cliniche anche esclusivamente in modalità digitale.

Prenotazioni e pagamenti online

- Il Ministero della salute ha emanato le "Linee guida nazionali - Sistema Centri Unici di Prenotazione - CUP"; tutte le regioni e province autonome stanno operando al fine di integrare i sistemi CUP esistenti a livello locale.
- Il D.M. 8 luglio 2011 del Ministero della salute regola l'erogazione, da parte delle farmacie, di attività di prenotazione delle prestazioni di assistenza specialistica ambulatoriale, il pagamento delle relative quote di partecipazione alla spesa a carico del cittadino e il ritiro dei referti relativi a prestazioni di assistenza specialistica ambulatoriale, da attuare con previsione nell'accordo collettivo nazionale.
- Il D.L. 13 maggio 2011, n. 70, ha introdotto l'obbligo di accettare pagamenti elettronici per tutte le aziende sanitarie (DPCM attuativo 8 agosto 2013). L'obbligo per tutte le pubbliche amministrazioni di consentire agli utenti pagamenti in modalità elettronica è inoltre previsto (a decorrere dal 1 giugno 2015) dall'articolo 5 del CAD, integralmente modificato dal DL 179/2012.
- Il D.L. 9 febbraio 2012, n.5, "Semplifica Italia" (art. 47-bis), promuove la gestione elettronica delle prenotazioni alle prestazioni sanitarie.

Calcolo dei benefici

Si tratta di iniziative in grado di determinare consistenti risparmi sulla spesa pubblica. Il Politecnico di Milano, ad esempio, stima che le strutture sanitarie potrebbero risparmiare circa 3,8 miliardi l'anno: circa 2,2 miliardi grazie al FSE, alla cartella clinica elettronica e alla dematerializzazione dei referti (per risparmi di tempo in attività mediche e infermieristiche e riduzione di sprechi dovuti alla stampa); oltre 800 milioni grazie alla riduzione di ricoveri dovuti a errori evitabili attraverso sistemi di gestione informatizzata dei farmaci; circa 400 milioni di euro grazie alla consegna dei referti via web e a un miglior utilizzo degli operatori dello sportello; 160 milioni con la prenotazione online delle prestazioni; 150 milioni attraverso la razionalizzazione dei data center presenti sul territorio e al progressivo utilizzo di tecniche di virtualizzazione.
A questi benefici, il Politecnico di Milano osserva che sono da aggiungere i possibili risparmi economici per i cittadini, grazie al miglioramento del livello di servizio, stimabili complessivamente in circa 5,4 miliardi di euro:
4,6 miliardi di euro dovuti alla possibilità di ritirare referti via web; oltre 600 milioni di euro grazie alla prenotazione via web e telefonica delle prestazioni; 170 milioni di euro grazie alle soluzioni di gestione informatizzata dei farmaci.
Investire in sanità elettronica significa inoltre investire nelle infrastrutture abilitanti allo sviluppo del paese: la domanda indotta (di banda larga, contenuti e servizi ICT) è stimata in 400 Meuro annui nel breve periodo, 1 Mld euro annui nel medio periodo e 2 Mld euro annui nel lungo periodo.

3. I riferimenti normativi

Di seguito alcuni interventi nazionali normativi e di indirizzo tecnologico di rilevante impatto per il mondo della sanità digitale, in generale, e per il Fascicolo Sanitario Elettronico in particolare. Alcuni di essi sono:

- D.L. 18 ottobre 2012, n. 179, recante “Ulteriori misure urgenti per la crescita del Paese” (convertito, con modificazioni, dalla L. 17 dicembre 2012, n. 221), ha istituito il Fascicolo Sanitario Elettronico (FSE);
- D.L. 21 giugno 2013, n. 69, recante “Disposizioni urgenti per il rilancio dell’economia” (convertito, con modificazioni, dalla L. 9 agosto 2013, n.98) di modifica al D.L. n. 179/2012;
- DPCM n.178 del 29 settembre 2015, pubblicato sulla G.U. dell'11 novembre 2015, n. 263, che ha emanato il "Regolamento in materia di fascicolo sanitario elettronico.";
- DPCM n.14 novembre 2015, pubblicato sulla Gazzetta ufficiale n.303 del 31 dicembre 2015, che definisce le "modalità di attuazione del comma 2 dell'articolo 13 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modifiche, dalla legge 17 dicembre 2012, n. 221, in materia di prescrizioni farmaceutiche in formato digitale", in vigore dal 1° gennaio 2016";
- DM 9 Dicembre 2015 "Condizioni di erogabilità e indicazioni di appropriatezza prescrittiva delle prestazioni di assistenza ambulatoriale erogabili nell'ambito del Servizio sanitario nazionale.", pubblicato sulla Gazzetta ufficiale n.15 del 20 gennaio 2016;
- Nuove Pubblicazioni e aggiornamenti documentali del Progetto TS (Tessera Sanitaria) con riguardo a sistema di accoglienza centrale (SAC) in ossequio alle disposizioni di cui all'articolo 50 della Legge 24 novembre 2003 n. 326 e dai suoi decreti attuativi;

- Piano Triennale per l'Informatica nella Pubblica amministrazione 2017 – 2019 approvato il 31/05/2017 dal Presidente del Consiglio dei Ministri e realizzato da AgID e dal Team per la Trasformazione Digitale;
- Linee guida per la presentazione dei piani di progetto regionali per il FSE;
- La Delibera di Giunta Regionale n. 559 del 17/9/2017;
- La Delibera di Giunta Regionale n. 25 del 18/01/2018;
- Il Decreto commissariale n. 26 del 22/2/2019;

4. Lo Stato dell'arte in Regione Campania e le azioni in corso

In Regione Campania è particolarmente evidente la frammentazione dei software presenti all'interno delle Aziende Sanitarie Locali e Ospedaliere, tanto che risulta indispensabile attuare interventi strutturali e radicali, al fine di uniformare la risposta informativa, di garantire idonei livelli di "data protection" e di disponibilità dei servizi sia all'interno dell'infrastruttura dei datacenter delle Aziende Sanitarie che dei servizi a livello regionale, attraverso un potenziamento dei livelli di sicurezza e resilienza dei sistemi.

La parcellizzazione dei sistemi software, delle banche dati, dei fornitori e, non ultimo, dei modelli organizzativi adottati dalle singole aziende, determina un panorama quanto mai affastellato, con ricadute molto negative anche e soprattutto sul livello regionale, che non ha la possibilità di essere il catalizzatore naturale dei flussi informativi e dei processi produttivi clinici e amministrativi che dovrebbero contribuire a generare conoscenza sul livello di qualità e quantità dei servizi sanitari erogati.

Le linee Guida per la presentazione dei Piani di progetto regionale per il Fascicolo Sanitario regionale e predisposte dall'Agenzia per l'Italia Digitale (AgID), ai sensi dell'art. 12 del D.L. 179/2012, prevedono quale componente abilitante per la realizzazione del FSE, la presenza di anagrafi degli assistiti, degli operatori e delle strutture di livello centrale regionale.

In ottemperanza a quanto richiesto dalle linee guida, la Giunta Regionale ha approvato la deliberazione n° 25 del 23/01/2018 con cui, tra l'altro, si prevede la razionalizzazione dei sistemi informativi sanitari regionali, attraverso l'unificazione e centralizzazione delle anagrafi di tutte le aziende sanitarie, al fine di rendere certificata ogni singola posizione anagrafica nel sistema regionale. Il sistema regionale dovrà inoltre allinearsi con il sistema nazionale di controllo della spesa farmaceutica e specialistica (Sistema TS) gestito dal Ministero delle Entrate e delle Finanze e con le nascenti Anagrafe Nazionale della Popolazione Residente (ANPR) e Anagrafe Nazionale degli Assistiti (ANA).

4.1 SINFONIA – Sistema INFOrmativo saNità campanIA

Tutti i Sistemi Sanitari Regionali, oggi, devono agire di concerto con le indicazioni dell'Agenzia per l'Italia digitale. L'utilizzo di nuove piattaforme favorisce, infatti, lo snellimento delle procedure e porta vantaggi a tutti gli attori e gli ambienti della sanità, valorizzando nel contempo le eccellenze sul territorio.

SINFONIA, **S**istema **INFO**rmativo sa**N**ità Campan**IA**, è il sistema informativo sanitario regionale al servizio degli utenti e degli operatori (in coerenza col piano 2017-2019 per l'informatica nella

Pubblica Amministrazione) progettato per supportare l'intero governo del SSR campano, aumentare l'efficienza, contenere i costi e al tempo stesso potenziare la risposta ai bisogni di tutti i protagonisti del sistema, operatori, cittadini, strutture, referenti dell'ente regionale e dell'amministrazione centrale.

Con l'adozione di SINFONIA il sistema della sanità campana passa dall'autonomia delle ASL alla gestione integrata del comparto sul territorio, operando un'innovativa pianificazione delle risorse di settore che fa crescere esponenzialmente quantità e qualità delle funzioni, con l'obiettivo di sostenere le eccellenze della sanità operativa, attraverso le opportunità della sanità digitale.

L'architettura di sistema web-based estende i vantaggi del digitale alla gestione di specifiche aree operative:

- Anagrafe Regionale degli Assistiti
- Anagrafe Regionale Strutture Sanitarie
- Anagrafe Regionale del personale SSR
- Gestione dei Medici di Medicina Generale e dei Pediatri
- Mobilità Sanitaria
- Gestione dei flussi informativi

L'intero settore regionale si avvantaggerà dell'utilizzo di SINFONIA, poiché la piattaforma permette l'analisi del fenomeno sanitario nella sua completezza attraverso la gestione di un'enorme quantità di dati e di flussi.

Ciò consente di armonizzare l'incontro tra l'offerta e la domanda, proporre nuovi modelli assistenziali e così ottimizzare la spesa farmaceutica e ospedaliera, migliorando i servizi territoriali in accordo con il Piano Regionale.

Snodo cruciale del progetto è un'innovativa concezione delle anagrafi sanitarie concernenti assistiti, operatori e strutture. L'architettura di sistema è concepita per incrociare necessità e disponibilità all'interno di una cabina di regia centrale e quindi consente risposte immediate a ogni esigenza di settore.

A ciò si aggiunge il progressivo miglioramento dei livelli di assistenza che la Regione potrà offrire, conoscendo in maniera più ampia e dettagliata il profilo dei propri assistiti, l'epidemiologia territoriale, le statistiche analitiche dell'offerta, delle prestazioni e dei livelli di successo resi dall'intero comparto.

Non secondario è l'accrescimento dello spirito partecipativo a un progetto comune. Il tema principale di SINFONIA è la cooperazione di tutte le figure del comparto, al fine di eccellere nel proprio settore sentendosi parte integrante di un organismo composito ma unito nel rispondere ai bisogni dei cittadini.

La piattaforma mette in comunicazione tutto il network di operatori facenti capo alle aziende sanitarie pubbliche, alle strutture accreditate, agli uffici della sanità campana e ad altri organismi regionali, permettendo loro di operare come fornitori e fruitori di informazioni.

Fanno parte della rete:

- Gestori dei rapporti con i medici convenzionati
- Operatori dei servizi di anagrafe sanitaria

- Medici di medicina generale e pediatri di libera scelta, medici specialisti, medici di continuità assistenziale, medici di medicina dei servizi e di emergenza territoriale
- Medici prescrittori ed erogatori di prestazioni sanitarie
- Unità di valutazione multidisciplinare dell'assistenza territoriale
- Responsabili di distretto, di unità operative, top management delle aziende
- Operatori sanitari di enti privati accreditati - Uffici di gestione del personale, gestione economica, del patrimonio, tecnica e di assistenza farmaceutica, di controllo gestione, di epidemiologia e statistica.

Il progetto denominato **S**istema **INFO**rmativo sa**N**ità Campan**IA** – **SINFONIA** prevede la costituzione di:

1. **Anagrafe Regionale Assistiti**: si basa, come tutti i modelli di sanità elettronica, sul concetto di "paziente al centro". L'Anagrafe Regionale degli Assistiti rappresenta uno snodo centrale di tutte le informazioni di carattere anagrafico-sanitario dei cittadini su cui si appoggiano i servizi gestionali e di riconoscimento dell'assistito, rilascio TS, scelta e revoca del medico, di esenzione, ecc. L'area centralizza il data base regionale eliminando le anagrafi ASL e ne consente l'aggiornamento in tempo reale incrociando i dati rivenienti da Anagrafe della Popolazione Residente (APR) e Sistema TS (Tessera Sanitaria). Trasferimenti, cambi di residenza, decessi, iscrizioni, scelte e revoche, esenzioni ticket, assistenza all'estero e altro sono gestiti univocamente dal sistema. Saranno così snelliti i passaggi burocratici legati alle posizioni di assistiti deceduti e rimasti in carico al medico di base, assistiti adolescenti ancora in carico al pediatra, esenzioni da rilasciare o da ritirare e così via, con grande risparmio di risorse. Le funzioni ARA sono articolate, ma razionali e di facile uso. A grandi linee governano:
   - Iscrizioni e variazioni
   - Scelta e revoca del medico di base e del pediatra di libera scelta
   - Esenzioni ticket
   - Assistenza all'estero per i cittadini italiani in paesi convenzionati
   - Rapporti con i centri di altissima specializzazione in paesi esteri
   - Stranieri temporaneamente presenti sul territorio
   - Allineamento tra Anagrafe Assistiti SSR e Anagrafe Ministero Economia e Finanze
   - Integrazione con altri sistemi esterni.
2. **Anagrafe Regionale delle Strutture Sanitarie e Socio-Sanitarie**: contiene l'anagrafica di tutte le strutture sanitarie, pubbliche e private accreditate della Regione. Essa consente di assolvere agli adempimenti della legge 326/2003 – articolo 50 e di catalogare in modo strutturato, tutte le strutture sanitarie regionali, i servizi disponibili, nonché tutte le informazioni utili per i cittadini e per gli operatori della sanità. L'archivio può essere agganciato anche ai sistemi regionali di georeferenziazione e svolge le seguenti funzioni:
   - viene referenziato dai servizi applicativi sanitari e socio-sanitarie e dalle applicazioni che gestiscono dati relativi alle strutture sanitarie regionali;

- costituisce la fonte delle informazioni per la programmazione sanitaria regionale, grazie alle informazioni presenti sull'offerta dei servizi (posti letto, tipologie di prestazioni erogate, ecc.);
- risponde a quanto previsto dal sistema nazionale di Monitoraggio della Rete di Assistenza (MRA);
- fornisce i contenuti per la gestione dinamica di un portale sanitario regionale dedicato.

L'anagrafe assistiti viene interfacciata con l'ARSS relativa alle strutture (aziende, distretti, ospedali, studi medici, cliniche, farmacie etc.) per una più snella e veloce erogazione dei servizi. L'anagrafe centralizzata avvantaggia sia gli operatori sia i cittadini, poiché razionalizza le prestazioni sul territorio e fornisce agli utenti informazioni circa l'offerta, la dislocazione, la logistica di queste strutture.

L'ARSS organizza i dati per:

- Classificazione, gestione e variazioni delle strutture sanitarie regionali
- Gestione degli istituti di ricovero e delle strutture trasfusionali fuori regione.

3. **Anagrafe Regionale del personale SSR**: comprende tutti gli operatori sanitari che interagiscono nel sistema e che appartengono al sistema sanitario regionale, sia che essi lavorino in ambito pubblico, sia che essi lavorino in ambito privato. L'anagrafe deve fornire un insieme di servizi di identificazione del ruolo e dell'incarico che l'operatore svolge in una determinata azienda/struttura (anche ambulatoriale) e contestualmente al tempo a cui la richiesta di tale informazione si riferisce. Tali informazioni possono essere usate per profilare gli operatori sui diritti di accesso in lettura e scrittura ai sistemi in uso e per fornire un attributo di ruolo da associare ai certificati per la firma digitale. L'anagrafe deve contenere informazioni riguardanti la persona fisica e alla struttura di competenza.

   La complessità logistico-amministrativa del mondo del lavoro trova soluzioni razionali in quest'area che si occupa interamente del rapporto con le risorse umane, gestendo per ciascun dipendente i dati anagrafici, i dati dei rapporti di lavoro, le unità operative di servizio, i costi. Questi dati sono poi trasferiti a tutti gli Enti superiori competenti.

   L'AR-PSSR governa quindi:

   - Gestione anagrafe del personale
   - Gestione delle dotazioni organiche
   - Simulazione costi del personale
   - Produzione dei ruoli nominativi regionali
   - Produzione dei flussi informativi verso il Ministero della salute, l'Assessorato alla sanità.

   La gestione e il controllo dei rapporti amministrativi e contabili con i medici di MG e i pediatri LS è un altro tassello importante del processo, poiché esso supporta gli enti deputati nel rapporto con il corpo sanitario di base. Le procedure consentono, inoltre, ai medici l'interazione con il sistema per aggiornare la propria posizione anagrafica, segnalare sostituzioni, comunicare le interruzioni operative, registrare le attività accessorie (visite occasionali, bilanci di salute, prestazioni speciali etc.).

   Le funzionalità riguardano:

- Gestione graduatorie regionali della Medicina Generale
- Gestione incarichi e convenzionamento
- Calcolo automatico delle competenze sulla base degli assistiti in carico, degli arretrati, delle competenze accessorie
- Calcolo automatico delle indennità
- Gestione dei fondi contrattuali nazionali, regionali ed aziendali
- Calcolo automatico degli emolumenti da accordi di livello regionale
- Gestione dei rapporti fiscali e previdenziali, procure all'incasso, cessioni
- Gestione completa delle forme associative da ACN nazionali e regionali.

Attraverso SINFONIA il professionista può inoltre ricevere cedolini paga e certificazioni fiscali, prelevare in autonomia gli elenchi relativi agli assistiti, alle scelte, alle revoche e alle esenzioni ticket, nonché caricare nel sistema visite occasionali, prestazioni PIPP, dati e orari degli studi e degli ambulatori. Il sistema può gestire l'integrazione diretta mediante Web Service con i software degli studi medici, per la trasmissione dati in tempo reale.

4. **Mobilità sanitaria**: obiettivo di questa area è supportare tutti gli operatori riconducibili alla sanità regionale nei processi di:
    - Compensazione per la mobilità sanitaria attiva e passiva intraregionale, interregionale e internazionale
    - Gestione di mobilità sanitaria dei cittadini stranieri, interfacciandosi anche coi sistemi del Ministero della Salute
    - Messa a disposizione di tutti i report previsti dalla normativa in vigore, utili alla richiesta del relativo rimborso.

    Particolare rilievo merita la gestione della mobilità sanitaria interregionale attiva e passiva, che consente alla sanità campana la valorizzazione delle prestazioni da addebitare alle altre Regioni e il controllo di quelle da erogare ad assistiti extraregionali, gestendo anche contestazioni e controdeduzioni.

    La gestione della mobilità sanitaria intraregionale eroga i medesimi servizi in riferimento ai cittadini residenti in Campania, mentre la gestione della mobilità sanitaria internazionale attiva e passiva cura le prestazioni erogate a cittadini stranieri non iscritti, privi di permesso o appartenenti a paesi non convenzionati. È prevista anche la gestione dei trasferimenti all'estero per cure di alta specializzazione, la produzione dei report previsti dalla normativa e la produzione di statistiche, al fine di fornire alle politiche regionali bussole affidabili per la programmazione sanitaria.
5. **Gestione flussi informativi**: la più grande opportunità della piattaforma SINFONIA è il controllo di dati statistici rilevanti, il cui movimento in ingresso o in uscita richiede risorse importanti sia sul versante dell'efficienza sia su quello della sicurezza. La disponibilità di dati validati ed aggiornati rappresenta uno strumento indispensabile per la programmazione e il controllo del SSR e il governo e la gestione della spesa, ai fini della verifica del grado di raggiungimento degli obiettivi regionali e del Piano di Rientro. Il sistema ottimizza la raccolta dei flussi informativi dalle Aziende Sanitarie e l'inoltro unificato attraverso il cruscotto di gestione verso il Ministero della Salute (N-SIS), il

Ministero Economia e Finanze (Sistema TS), l'ISTAT, etc. I flussi riguardano tutti i molteplici aspetti della sanità, dalla dematerializzazione delle ricette al tesseramento individuale, alla farmaceutica, al pronto soccorso, all'assistenza residenziale o domiciliare, alla salute mentale, alla specialistica, alla mobilità e molto altro.

4.2 Il Fascicolo Sanitario Elettronico Regionale

Nell'ecosistema Sanità, un ruolo centrale è ricoperto dal **Fascicolo sanitario elettronico (FSE)** che è lo strumento attraverso il quale il cittadino può tracciare, consultare e condividere la propria storia sanitaria. La norma stabilisce che l'infrastruttura del FSE gestisca l'insieme dei dati e dei documenti digitali di tipo sanitario e socio-sanitario, generati da eventi clinici presenti e trascorsi riguardanti l'assistito.

La Legge di Bilancio 2017, al fine di assicurare un'omogenea diffusione nazionale del FSE, ha variato il quadro di riferimento per gli scenari di evoluzione e diffusione del FSE con l'introduzione dell'Infrastruttura Nazionale per l'Interoperabilità (INI) dei Fascicoli Sanitari Elettronici regionali, nonché con la revisione di adempimenti e scadenze previsti per la realizzazione dei progetti di FSE da parte delle Regioni. Fermo restando quanto già previsto nell'ambito del D.P.C.M. n. 178 del 29/9/2015 "Regolamento in materia di fascicolo sanitario elettronico" e dalle specifiche AgID per l'interoperabilità tra i sistemi regionali di FSE, l'INI ha il compito di garantire l'interoperabilità dei FSE regionali e mette a disposizione una serie di funzionalità per l'alimentazione e la consultazione del FSE. L'infrastruttura nazionale, oltre a garantire i processi operativi per sistemi regionali di FSE esistenti, dovrà assicurare funzioni, nella loro interezza o in maniera modulare, per la realizzazione e gestione di un sistema di FSE per le regioni e province autonome che non hanno sviluppato completamente proprie soluzioni di FSE. (regime di sussidiarietà)[2] INI espone dei servizi che si possono suddividere nelle seguenti macro categorie:

- servizi di gestione e comunicazione dei consensi;
- servizi di gestione e comunicazione delle informative regionali;
- servizi di recupero dei metadati dei documenti che compongono il FSE;
- servizi di recupero dei documenti del FSE, compatibilmente con le politiche di accesso da parte di un assistito, un operatore o un professionista sanitario;
- servizi di comunicazione o di aggiornamento dei metadati relativi ad un documento o di cancellazione dei metadati di un documento invalidato;
- servizio di trasferimento dell'indice a seguito del cambio della regione di assistenza di un assistito.

La Regione Campania ha aderito in toto all'infrastruttura nazionale di sussidiarietà. INI ha messo a disposizione di queste Regioni le principali componenti di storage dell'infrastruttura (repository e registry) e alcuni servizi tra cui:

- Autenticazione cittadini e professionisti sanitari;
- Gestione del consenso e oscuramenti documenti;
- Comunicazione dell'informativa;
- Consultazione FSE;

[2] Conferenza Stato regioni, Contributo sullo stato di attuazione del FSE, 26 ottobre 2017.

- Indicizzazione documenti;
- Archiviazione documenti;
- Consultazione accessi;
- Gestione e indicizzazione dei patient summary

Inoltre, ad integrazione dei contenuti minimi previsti dal DPCM 178/2015 (dati identificativi e amministrativi dell'assistito, referti, verbali pronto soccorso, lettere di dimissione, profilo sanitario sintetico, dossier farmaceutico, consenso o diniego alla donazione degli organi e tessuti), nell'ambito delle attività del Tavolo di monitoraggio FSE sono stati individuati come prioritari anche i seguenti contenuti:

- prescrizioni (specialistiche, farmaceutiche, ecc.);
- bilanci di salute;
- dossier farmaceutico;
- vaccinazioni;
- prestazioni di assistenza specialistica;
- certificati medici;
- esenzioni;
- prestazioni di assistenza protesica;
- promemoria ricetta.

I documenti e le informazioni cliniche, di cui sopra, dovranno prevedere i contenuti minimi ed essere resi disponibili in formato CDA2 secondo le specifiche che saranno prodotte dai gruppi di lavoro *ad hoc* recentemente costituiti nell'ambito dei tavoli tecnici nazionali (GDL).

Dal quadro di contesto sintetizzato in precedenza, discendono per le Regioni una serie di attività da porre in essere che sono sistematicamente monitorate dal livello nazionale.

Anche la Regione Campania, pur avendo aderito al regime di sussidiarietà, ha posto in essere un complesso coordinato di attività propedeutiche per adempiere alla normativa e popolare il FSE-INI. Tali attività sono volte a:

- creare le condizioni perché il FSE possa essere alimentato in modo completo, corretto e continuativo dalle strutture che producono i documenti, gestendo in modo coordinato il percorso di adeguamento tecnico ed organizzativo delle strutture stesse, pubbliche e private.
- definire le strategie di coinvolgimento degli operatori in senso lato (MMG, PLS, farmacie…) nel percorso di attivazione del fascicolo;
- coordinare le attività di promozione e formazione rivolte a cittadini e operatori.

Il Piano Triennale per l'informatica nella Pubblica Amministrazione 2017 – 2019 è articolato in diversi capitoli tematici tra i quali è presente quello dedicato agli Ecosistemi interoperabili e in particolare quello sull'Ecosistema Sanità. Nel piano viene illustrato il modello strategico ed operativo di riferimento per lo sviluppo e l'evoluzione del sistema informativo sanitario puntando l'attenzione sullo strumento "cardine" del Fascicolo Sanitario Elettronico quale strumento attraverso il quale il cittadino può tracciare, consultare e condividere la propria storia sanitaria attraverso una infrastruttura che gestisce l'insieme dei dati e dei documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi riguardanti l'assistito.

Il FSE, implementato secondo una visione strategica e una progettualità di ampio respiro, è uno strumento che facilita l'erogazione e l'accesso ai servizi sanitari sfruttando le potenzialità del digitale e riesce ad avvicinare i servizi ai bisogni dei cittadini e professionisti della salute. In quest'ottica la regione intende realizzare un cambio di paradigma in cui il FSE è molto di più di un contenitore di documenti e dati clinici, è una nuvola integrata di dati da utilizzare per la costruzione di servizi ad alto valore aggiunto:

- per il paziente, accompagnandolo lungo tutto il percorso di cura, rendendo facile l'accesso ai servizi sia per lui che per i suoi familiari anche attraverso canali innovativi e digitali, migliorando l'esperienza d'uso dei servizi offerti;
- per i professionisti e gli operatori del settore: valorizzando la rete e lo scambio di informazioni, finalizzato a promuovere la condivisione delle esperienze ed un approccio multidisciplinare al paziente;
- per la Regione stessa, in quanto promuove l'efficienza del sistema attraverso la riorganizzazione e la dematerializzazione dei processi e mette a disposizione un corredo di dati clinici per il governo del sistema, eventualmente da condividere con attori terzi in una logica di "open data".

4.3 Le altre componenti regionali

Le altre soluzioni in corso di realizzazione sono: il **Centro unico di prenotazione (CUP)**, il sistema centralizzato informatizzato per la prenotazione unificata delle prestazioni, per favorire l'accessibilità dell'assistenza e la riduzione dei tempi di attesa; il cruscotto regionale per le liste di attesa, l'anagrafe vaccinale, la dematerializzazione della **cartella clinica** e la consultazione online tramite il fascicolo sanitario elettronico, il progetto **Telemedicina** per offrire servizi che migliorino la fruibilità delle cure, dei servizi di diagnosi e della consulenza medica a distanza, oltre al costante monitoraggio di parametri vitali.

4.3.1 Centro unico di prenotazione (CUP)

Il Decreto del Commissario ad Acta n. 134 del 28 ottobre 2016, alla linea progettuale 2, ha previsto la creazione di un CUP regionale per la gestione delle prenotazioni e l'abbattimento delle liste di attesa. In continuità, anche con quanto previsto dai Programmi Operativi 2016-2018 approvati con il Decreto Commissariale n. 14 del 1 marzo 2017, è stata prevista la progettazione di un CUP regionale.

Al fine di consentire una fase di progettazione che fosse la più aderente possibile alle esigenze del territorio, La Direzione Generale per la Tutela della salute e il Coordinamento del Sistema Sanitario regionale ha coinvolto i responsabili dei CUP aziendali ed i loro referenti informatici, al fine di relazionare sulle modalità di raccolta dei flussi informativi e sull'adesione a quanto previsto dalle Linee Guida ministeriali.

Sulla base delle risultanze emerse dalla ricognizione effettuata dalla Direzione Generale, tenuto conto dell'esperienza maturata, è emersa la forte necessità di dotare la Regione Campania di un sistema CUP regionale che sia assolutamente compliant con il modello di riferimento nazionale e che consenta una visione completa e unificata della rete di offerta dei servizi sanitari, così come previsto dalle Linee guida nazionali, predisposte dal Ministero della salute, in collaborazione con le Regioni e su cui è stata acquisita, il 29 aprile 2010, l'Intesa della Conferenza Stato-Regioni (Intesa

tra il Governo, le Regioni e le Province autonome di Trento e Bolzano concernente il documento recante “Sistema CUP – Linee guida nazionali”. Rep. Atti n. 52/CSR del 29 aprile 2010). Tali Linee guida sono finalizzate proprio all’armonizzazione dei sistemi CUP, attraverso la definizione di caratteristiche minime ed uniformi relative a tali sistemi a livello nazionale.
La sintesi della ricognizione ha evidenziato, inoltre, elementi sia positivi che negativi. Mentre negli aspetti positivi si rileva una tendenziale rispondenza dei sistemi CUP di tutte le aziende sanitarie ed ospedaliere con gli obiettivi posti dalle linee guida in termini di gestione e programmazione delle agende di prenotazione e di accesso ai servizi e gestione del processo di prenotazione, nel contempo si evidenzia come la presenza di 17 sistemi CUP (7 ASL e 10 AOU) determini sicuramente uno svantaggio per i cittadini che non hanno un unico riferimento per prenotare prestazioni sanitarie presso strutture che insistono sul medesimo territorio o comunque su territori omogenei e/o limitrofi. Inoltre occorre evidenziare le diseconomie determinate dalla presenza di sistemi molto simili nelle funzioni (a volte erogati dallo stesso fornitore), ma che non riescono a comunicare, non tanto per impedimenti tecnologici, quanto per limiti organizzativi interaziendali.
Come previsto anche dalle Linee guida nazionali e dalle realtà regionali che hanno già implementato un CUP regionale, esistono due possibili soluzioni correntemente adottate, CUP unificato e CUP integrato, che permettono di realizzare un sistema di prenotazione a valenza regionale. Non si tratta solo di una distinzione rispetto alle soluzioni tecniche, ma anche di un diverso metodo di applicazione delle finalità di interazione e standardizzazione delle attività del CUP all'interno di un contesto territoriale. Diverse sono le motivazioni che possono portare alla prevalenza di un modello realizzativo sull'altro come sono diversi i vantaggi e gli svantaggi delle possibili soluzioni. Entrambi i modelli, tuttavia, prevedono un coordinamento interaziendale a livello regionale e la possibilità di accentrare specifici ambiti d'attività del CUP, allo scopo di beneficiare di economie di scala e di specializzazione delle figure coinvolte all'interno di ambiti cruciali d'attività (quali, ad esempio, la gestione delle agende e della prenotazione telefonica, delle regole comportamentali, ecc.).
Il filo conduttore nell’implementazione del CUP regionale campano è di rendere disponibile la prenotazione delle prestazioni sanitarie in "circolarità", cioè tramite tutti i punti d'accesso del Sistema CUP, indipendentemente dall'appartenenza a una specifica Azienda Sanitaria, nel rispetto dell’ambito territoriale di garanzia previsto per quella tipologia di prestazione per i propri assistiti.
È in questo contesto che si inserisce la scelta di Regione Campania sul modello di CUP da realizzare. Nello specifico il disegno del Sistema CUP Campano può essere così schematizzato:

- 1° livello: CUP Provinciali. È il primo di livello di accesso per i cittadini, che potranno prenotare le prestazioni sanitarie presso una qualunque struttura sanitaria appartenente al SSN o alle strutture private accreditate (che entrano a far parte del circuito del CUP), inserite nel contesto territoriale di appartenenza del cittadino. Il primo livello cercherà di contemperare sia la celerità di erogazione della prestazione che il rispetto del vincolo territoriale.
- 2° livello: CUP regionale. Nel caso non siano disponibili strutture sanitarie (sia SSN che del privato accreditato), che possano erogare le prestazioni in tempi compatibili con quelli previsti dalla legge, saranno prospettate al cittadino una serie di possibili alternative, che

terranno conto sia del contesto territoriale che del rispetto delle liste di attesa, attingendo dall'elenco delle strutture comunque prossime geograficamente rispetto alla residenza del cittadino. Il 2° livello potrà essere utilizzato anche nel caso in cui sia il cittadino a chiedere espressamente l'erogazione presso altra ASL/AO fuori dal territorio provinciale (ad esempio lavoratori pendolari che per ragioni di lavoro trovano più semplice ottenere la prestazione vicino al luogo di lavoro piuttosto che a quello di residenza).

- Coordinamento regionale: la governance sui CUP sarà centralizzata, soprattutto in materia di monitoraggio delle liste di attesa. La regia regionale sarà garantita dall'utilizzo di una piattaforma unica di prenotazione regionale, che consentirà di avere dati uniformi, coerenti, completi e soprattutto in tempo reale. In questo modo sarà possibile attuare misure di politica sanitaria mirate e basate su dati oggettivi.

4.3.2 Anagrafe Vaccinale Regionale

La Regione Campania ha aderito alla legge sugli obblighi vaccinali n.119 del 31 luglio 2017, istituendo l'anagrafe unica vaccinale che raccoglie i dati di informatizzati di tutti i nuovi nati dal 2001 al 2018 (ubicata presso SO.RE.SA. SPA).

Gli obiettivi perseguiti con l'istituzione dell'anagrafe vaccinale sono stati:

- Centralizzazione delle funzioni di controllo e monitoraggio
- Uniformità nell'erogazione dei servizi sull'intero territorio regionale
- Disponibilità dei dati sulla copertura vaccinale in tempo reale
    - sia a livello centrale che di singola ASL
    - in formati uniformi e standardizzati
- Semplificazione delle procedure di gestione degli applicativi
    - una sola piattaforma da configurare
    - una sola piattaforma da integrare
    - una sola piattaforma da manutenere
- Adozione di una piattaforma semplice ed intuitiva (GEVA, già adoperato in 5 ASL)

L'evoluzione della piattaforma ha consentito di:

- Adeguare la piattaforma GEVA, pensata per unità locali, al fine di:
    - gestire le banche dati in ottica multiaziendale
    - rendere intuitivo l'uso del sistema agli operatori di ogni ASL/centro vaccinale
- Assicurare uniformità nella rappresentazione delle informazioni
    - normalizzazione delle codifiche
    - Standardizzazione dei modelli regionali
    - migrazione dei dati storici
- Garantire agli operatori la possibilità di recuperare in tempo reale i dati relativi agli assistiti dell'intera Regione

La piattaforma ha consentito di facilitare il supporto alle comunicazioni Scuola – ASL.

Gli obiettivi perseguiti:

- Automatizzare lo scambio informativo per la verifica degli obblighi vaccinali degli assistiti in età scolastica (Legge 119 - 31 luglio 2017)
- Semplificare la verifica alle scuole ed il rilascio dei certificati alle ASL

- Agevolare gli operatori ASL nella verifica e recupero delle inadempienze
- Rendere le procedure di verifica trasparenti per i genitori degli assistiti
    - trasmissione diretta delle attestazioni di adempienza da ASL a scuole
    - convocazione dei genitori da parte dell'ASL solo in caso di inadempienza

4.3.3 Cruscotto regionale Liste di attesa

Con Decreto Commissariale n. 34 dell'8 agosto 2017 sono stati assegnati specifici obiettivi alle Aziende sanitarie per l'efficace governo dei tempi e delle liste di attesa.
In particolare, in ordine al governo delle liste di attesa, sono state emanate specifiche linee guida alle Aziende sanitarie per la riduzione dei tempi di attesa e sono stati definiti interventi più efficaci ed incisivi, da parte delle Aziende Sanitarie e della Direzione Generale per la Tutela della Salute e il Coordinamento del Sistema Sanitario regionale, fermi restando i principi e gli obiettivi di cui al PRGLA 2010-2012 approvato con la delibera di Giunta Regionale n. 271/2012 e, cioè: (i) le classi di priorità per le prestazioni di specialistica ambulatoriale e di ricovero ospedaliero programmato; (ii) i tempi massimi di attesa per ciascuna classe di priorità; (iii) le 43 prestazioni ambulatoriali, di cui 14 specialistiche e 29 di diagnostica strumentale, e le 15 prestazioni di ricovero ospedaliero programmato, di cui 5 in regime diurno e 10 in regime ordinario, per le quali sono fissati, garantiti e monitorati i tempi di attesa.
Al fine di monitorare costantemente lo stato delle liste di attesa di tutte le aziende sanitarie locali ed ospedaliere, è stato realizzato un cruscotto applicativo, basato su logiche di Business Intelligence, in grado di monitorare in maniera puntuale e/o in intervalli di tempo codificati le disponibilità e le performance delle liste di attesa di ciascuna azienda Sanitaria.
Il cruscotto, realizzato a partire dalla soluzione software di proprietà dell'Azienda Ospedaliera specialistica dei Colli, consente il monitoraggio:

a) dei temi di attesa reali e puntuali per le prestazioni sentinella
b) delle performance calcolate sulle prestazioni sentinella prenotate
c) delle performance calcolate sulle prestazioni sentinella erogate
d) dei ricoveri con diagnosi ed interventi sensibili.

Il cruscotto "**Prestazioni sentinella**" consente di monitorare, per le prestazioni individuate, i giorni di attesa per la prima disponibilità.
Nello specifico, il cruscotto, per ciascuna prestazione espone i seguenti valori:

a) Nome della prestazione e codice regionale;
b) Giorni di attesa per una fascia di priorità base (di solito B o D) per la prestazione indicata;
c) Data reale della prima disponibilità nel formato gg/mm/aa hh:mm;
d) L'agenda del CUP all'interno del quale è disponibile lo spazio per la prestazione;
e) Il plesso a cui fa riferimento l'agenda indicata.

I cruscotti relativi alle performance sono realizzati secondo le linee guide regionali e prevedono l'esposizione di un valore percentuale per ogni fascia di priorità. Le fasce di priorità per le prestazioni prenotabili attraverso il CUP sono: U (da erogare entro le 72 ore), B (da erogare entro 10 giorni), D (da erogare entro i 30 giorni per le prestazioni specialistiche e 60 giorni per le prestazioni strumentali), P (entro 180 giorni).

Nello specifico, questo cruscotto presenta le seguenti informazioni:

a) Nome e codice regionale della prestazione monitorata;
b) Per ciascuna fascia di priorità riporta i seguenti valori:
    i. **Performance**: è il rapporto, espresso in percentuale, tra il numero di prenotazioni per le quali la data di erogazione rientra nell'intervallo di tempo limite secondo quanto previsto dalle linee guida regionali ed il numero di prenotazioni per la quale la data di erogazione NON rientra nell'intervallo di tempo limite.
    ii. **Giorni di attesa**: è il numero medio di giorni di attesa relativo alle prenotazioni effettuate e non ancora erogate.
    iii. **Prenotati**: è il numero di prestazioni prenotate e non ancora erogate.

Il cruscotto delle "**performance per erogati**" è molto simile al cruscotto precedente ma tiene conto delle prestazioni erogate e non di quelle prenotate.
Nello specifico, questo cruscotto riporta le seguenti informazioni:

a) Nome e codice regionale della prestazione monitorata;
b) Per ciascuna fascia di priorità riporta i seguenti valori:
    i. **Performance**: è il rapporto, espresso in percentuale, tra il numero di prestazioni erogate nell'intervallo di tempo limite secondo quanto previsto dalle linee guida regionali ed il numero di prestazioni per le quali la data di erogazione NON rientra nell'intervallo di tempo limite.
    ii. **Giorni di attesa**: è il numero medio di giorni di attesa relativo alle prestazioni erogate.
    iii. **Dispersione**: è il numero di prestazioni prenotate ma per le quali il paziente non si è presentato oppure ha disdetto preventivamente l'appuntamento.
    iv. **Erogate**: indica il numero di prestazioni erogate in un intervallo di tempo codificato.

Il cruscotto relativo alle **performance relative ai ricoveri**, infine, monitora diagnosi ed interventi. Mentre i primi due cruscotti monitorano prestazioni specialistiche e strumentali prenotate attraverso il sistema CUP, questo cruscotto acquisisce i dati dal sistema ADT e dalle liste di attesa di ricovero.
Le fasce di priorità per il monitoraggio dei ricoveri sono: A (entro 30 giorni), B (entro 60 giorni), C (entro 180 giorni), D (entro un anno).
In dettaglio, il cruscotto presenta le seguenti informazioni:

a) Diagnosi e codice regionale;
b) Per ciascuna delle quattro priorità previste dalla regione, le seguenti informazioni:
    i. **Performance**: è il rapporto, espresso in percentuale, tra il numero di ricoveri effettuati entro il limite previsto dalle linee guida regionali per la specifica priorità ed il numero ricoveri avvenuto oltre il limite previsto.
    ii. **Giorni di attesa**: è la media dei giorni di attesa per i ricoveri effettuati in un intervallo di tempo codificato.

iii. **Pazienti in attesa**: è il numero di pazienti presenti in lista di attesa con la specifica diagnosi.

iv. **Pazienti erogati**: è il numero di ricoveri effettuati per la specifica diagnosi.

4.3.4 Cartella clinica elettronica

La dematerializzazione delle informazioni e dei dati della sanità (l'eHealth) è la condizione per una riorganizzazione etico-economica complessiva del settore. Essa è inoltre obiettivo indispensabile per una personalizzazione delle cure (sanità di precisione o di complessità) e per raggiungere nuovi traguardi nella ricerca clinica. Infine, la governance dell'ecosistema salute-sanità ha bisogno, oggi, di accogliere 'in tempo reale' i dati del rapporto domanda di salute – offerta di servizi (i *big data*), in un rapporto immediato con i cittadini, come si fa ormai in ogni Smart City.

La Regione Campania ha come obiettivo di realizzare/completare la parte 'verticale' del sistema (*Digital Hospital*), quella aziendale, con la completa dematerializzazione dei flussi informativi ospedalieri-ambulatoriali e la realizzazione di una Cartella Clinica Elettronica (CCE) 'verticale' (ambulatoriale e di reparto). Sotto questo aspetto occorre un particolare sforzo culturale per abbandonare il concetto di CCE come semplice dematerializzazione di quella cartacea in uso da oltre un secolo. Non si sostituisce solo "la carta" con "il digitale", ma si inserisce, piuttosto, un 'nodo' della rete eHealth: un EPR (Electronic Patient Record), interoperabile con ogni applicativo tecnologico dipartimentale, settoriale, di reparto, diagnostico. In sostanza un *Back End Temporale* del Dossier Sanitario Elettronico (cioè con la storia clicca del paziente a livello aziendale). La somma delle diverse cartelle cliniche dello stesso paziente generate nel tempo in un ospedale o in una azienda sanitaria diventa, così, di fatto, il Dossier Sanitario.

Il modello che si adotterà per la disseminazione delle cartelle cliniche elettroniche prevede la creazione di un catalogo dinamico di soluzioni che saranno "validate" e "abilitate" al mondo della sanità digitale campana. Questo consentirà di poter coprire tutte le esigenze, molto variegate, delle singole aziende, dipartimenti, ambulatori, preservando il requisito di base, l'integrazione e

5. Modello strategico di evoluzione del sistema informativo sanitario regionale[3]

Di seguito si ribadisce quanto previsto dal Piano Triennale per la Pubblica amministrazione dal punto di vista del Modello strategico da adottare, che risulta assolutamente in linea con quanto è indispensabile realizzare anche nel campo del SSR campano.

Il Modello strategico di evoluzione del sistema informativo della Pubblica amministrazione costituisce il quadro di riferimento su cui innestare e rendere operativi i progetti, le piattaforme e i programmi descritti nel documento Strategia per la crescita digitale 2014-2020 nel quale sono indicati i requisiti strategici da soddisfare, ovvero:

- facilitare il coordinamento di tutti gli interventi di trasformazione digitale e l'avvio di un percorso di centralizzazione della programmazione e della spesa pubblica in materia;

[3] https://pianotriennale-ict.readthedocs.io/it/latest/doc/02_modello-strategico-di-evoluzione-dell-ict-della-pa.html#modello-strategico-di-evoluzione-del-sistema-informativo-della-pubblica-amministrazione

- considerare prioritario il principio di "digitale per definizione" (*digital first*), progettando e implementando i servizi al cittadino, a partire dall'utilizzo delle tecnologie digitali;
- agevolare la modernizzazione della Pubblica amministrazione partendo dai processi, superando la logica delle regole tecniche e delle linee guida rigide emesse per legge. Esse dovranno essere dinamiche e moderne e puntare alla centralità dell'esperienza e ai bisogni dell'utenza;
- adottare un approccio architetturale basato sulla separazione dei livelli di *back end* e *front end*, con logiche aperte e standard pubblici che garantiscano ad altri attori, pubblici e privati, accessibilità e massima interoperabilità di dati e servizi;
- promuovere soluzioni volte a stimolare la riduzione dei costi e a migliorare la qualità dei servizi, contemplando meccanismi di remunerazione che possano anche incentivare i fornitori a perseguire forme sempre più innovative di composizione, erogazione e fruizione dei servizi.

La Strategia per la crescita digitale evidenzia la necessità di un radicale ripensamento della strategia di progettazione, gestione ed erogazione dei servizi pubblici in rete che preveda, tra l'altro, l'adozione delle architetture a più livelli (*multi-layer architecture*) e dei principi che hanno determinato l'affermazione del modello di business della cosiddetta *API economy*.

Il Modello strategico è stato quindi pensato per superare l'approccio a "silos" storicamente adottato dalla Pubblica amministrazione e per favorire la realizzazione di un vero e proprio sistema informativo della Pubblica amministrazione (di seguito "Sistema informativo della PA") che:

1. Consideri le esigenze dei cittadini e delle imprese come punto di partenza per l'individuazione e la realizzazione di servizi digitali moderni e innovativi (servizi di *front office*);
2. Uniformi e razionalizzi le infrastrutture e i servizi informatici utilizzati dalla Pubblica amministrazione (servizi di *back office*);
3. Favorisca la creazione di un nuovo mercato per quelle imprese private che saranno in grado di operare in maniera agile in un contesto non più basato su grossi progetti monolitici e isolati ma su servizi a valore aggiunto. Tali servizi dovranno (i) rispettare le linee guida del Piano triennale, (ii) essere sempre disponibili su dispositivi mobili (approccio mobile first) e (iii) essere costruiti con architetture sicure, scalabili, altamente affidabili e basate su interfacce applicative (API) chiaramente definite;
4. valorizzi le risorse esistenti della Pubblica amministrazione al fine di salvaguardare gli investimenti già realizzati, anche incoraggiando e creando le condizioni per il riuso del software e delle interfacce esistenti di qualità;
5. non disperda le esperienze maturate nei precedenti progetti di digitalizzazione del Paese con l'obiettivo di prendere a modello i casi di successo (*success stories*) e non ripetere errori commessi nel passato;
6. migliori la sicurezza grazie ad un'architettura a più livelli che assicuri la separazione tra back end e front end e permetta l'accesso ai back end solo in modo controllato e tramite API standard;

7. promuova la realizzazione di nuovi servizi secondo il principio di sussidiarietà (ad es. tramite interazioni API), riducendo tempi di realizzazione e impegni economici per le amministrazioni sia in fase di sviluppo sia in fase di aggiornamento;
8. agevoli il controllo delle spese relative alle tecnologie digitali della Pubblica amministrazione, integrando meccanismi per la misurazione dello stato di avanzamento delle attività programmate (ad es. tramite sistemi di project management condivisi);
9. abiliti politiche *data-driven* per la pianificazione delle attività future, basate sull'ottimizzazione delle spese e degli investimenti.

6. Le linee di indirizzo

Sulla base delle del modello strategico appena descritto, si elencano di seguito le linee di indirizzo, di carattere vincolante e prescrittivo, per la progettazione, sviluppo, implementazione, gestione e conduzione dei Sistemi Informativi Sanitari delle Aziende Sanitarie Locali e delle Aziende Ospedaliere appartenenti al Sistema Sanitario della Regione della Campania.
Le principali linee di intervento che dovranno necessariamente essere condotte e sviluppate sono così sintetizzate:

1. **La razionalizzazione dell'infrastruttura dei data center delle Aziende Sanitarie e la migrazione verso il Cloud**: tale attività si rende necessaria al fine di garantire idonei livelli di "data protection" e di disponibilità dei servizi che, a seguito della continua digitalizzazione dei processi clinico-assistenziali, si stanno progressivamente innalzando sia per gli effetti delle normative nazionali che per effetto della progettazione Regionale. [4] Un piano di razionalizzazione delle infrastrutture IT della Pubblica Amministrazione (PA) implica una visione di lungo periodo, importanti investimenti e un coordinamento che tenga conto delle varie realtà presenti sul territorio; sebbene si tratti di un percorso articolato e non del tutto agevole, i benefici che ne derivano garantiscono un ritorno non solo economico.
   Semplificare e razionalizzare l'architettura delle infrastrutture IT permette, infatti, di:
   1. creare ambienti più sicuri e affidabili;
   2. tenere sotto controllo con maggiore facilità i costi dell'IT (minori asset da gestire);
   3. contenere i costi di manutenzione e gestione, inclusi quelli relativi alla componente energetica;
   4. agevolare l'adozione di soluzioni SOA (Service Oriented Architecture);
   5. dimensionare in modo più rapido e flessibile le risorse software e hardware per far fronte ad esigenze non prevedibili o non continuative;
   6. prendere decisioni più consapevoli e pro futuro nella scelta di apparati IT e di software;
   7. standardizzare l'hardware, le applicazioni software e le modalità stesse di gestione dell'ICT;
   8. facilitare la cooperazione applicativa tra Amministrazioni.

[4] AgID - Linee Guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione

Le Infrastrutture fisiche oggetto della razionalizzazione sono, principalmente, gli *asset* hardware necessari per la realizzazione del servizio: le reti di comunicazione, i *data center*, il *cloud* della PA, i sistemi di *disaster recovery* e di *business continuity*, gli apparati per il monitoraggio e la sicurezza. Il piano di razionalizzazione deve svilupparsi lungo tre principali direttrici:

- la riorganizzazione del parco dei data center delle Aziende Sanitarie Locali e Aziende Ospedaliere, attraverso un'opera di razionalizzazione utile, sia a ridurre i costi di gestione, sia a uniformare e aumentare la qualità dei servizi offerti, anche in termini di *business continuity*, *disaster recovery* ed efficienza energetica;
- la realizzazione del *cloud* della Sanità campana, grazie al quale sarà possibile virtualizzare il parco macchine di tutte le Aziende, con importanti benefici in termini di costi e di gestione della manutenzione. I servizi *cloud* oggi offerti sono disponibili in modalità *IaaS* (*Infrastructure as a Service*), *PaaS* (*Platform as a Service*) e *SaaS* (*Software as a Service*);
- la razionalizzazione delle spese per la connettività delle Aziende.

Ciò comporta un diretto innalzamento dei livelli di sicurezza e di resilienza dei sistemi, sono azioni da considerare a priorità elevata, anche per ridurre significativamente gli investimenti delle singole aziende soprattutto in termini di presidii di supporto sistemistico. La necessità di razionalizzare i CED della Aziende Sanitarie non deve quindi essere messa in discussione, ma deve essere considerata come un'opportunità da cogliere e da cui non essere esclusi. Le Amministrazioni che potranno contare su CED più innovativi potranno offrire una qualità del servizio decisamente superiore. Un livello di qualità che tutta la PA deve pretendere per la conservazione e gestione dei propri dati, soprattutto in considerazione della straordinaria portata innovativa del cloud computing che ha completamente scardinato le modalità di approccio alle architetture IT.

2. **Connettività:** le Aziende sanitarie devono avviare processi di adeguamento della propria connettività al fine di poter erogare tutti i servizi relativi sia ai processi amministrativi interni sia ai servizi pubblici rivolti ai cittadini. Si dotano di un'infrastruttura di collegamento di rete in grado di rispondere almeno ai seguenti principi generali:
    - capacità di banda sufficiente a soddisfare i requisiti dei servizi IT interni ed erogati verso l'esterno;
    - livelli di servizio adeguati a garantire il funzionamento delle applicazioni utilizzate;
    - scalabilità della capacità di banda anche per erogazione di banda wi-fi per uso pubblico;
    - livelli di sicurezza conformi agli standard internazionali;
    - configurazioni di rete in alta affidabilità in caso di Infrastrutture critiche.
    - Le amministrazioni definiscono i parametri puntuali e il livello di affidabilità della rete in base allo specifico contesto applicativo, all'uso delle relative applicazioni e ai livelli di servizio offerti. Inoltre predispongono i propri servizi per supportare il protocollo IPv6.

La connettività Internet deve essere finalizzata a:

- garantire accesso alla rete Internet a tutti i dipendenti, indipendentemente dal ruolo o dai compiti assegnati e senza limiti di tempo o orari. Internet oggi deve essere considerato a tutti gli effetti uno strumento di lavoro indispensabile ed efficace per svolgere ogni tipo di attività: dal trovare numeri di telefono, all'identificare persone e relazioni tra queste persone, riferimenti di un concorso o normativi, documentazione tecnica, strumenti di produttività (traduzioni, orari nel mondo, ecc.), servizi di emergenza o notizie di ogni tipo.
- garantire accesso non solo agli strumenti ed alle applicazioni utilizzati dalla PA, ma - previa analisi delle necessità organizzative in relazione agli obiettivi da raggiungere - a tutti i contenuti e gli strumenti che Internet mette a disposizione, inclusi strumenti per la condivisione di file e contenuti, social network, nonché siti come forum, chat o altri strumenti di comunicazione.

Pertanto il potenziamento dell'infrastruttura di rete tra le strutture sanitarie si ritiene fondamentale e propedeutica al potenziamento e alla razionalizzazione dei data center di cui al punto precedente. Vista la natura altamente critica dei servizi erogati dalle strutture sanitarie e, rilevato che la mole di dati prodotti nei processi clinico-assistenziali è in continuo aumento (si pensi alle bio-immagini, alle ricette dematerializzate ed ai documenti clinici digitalizzati), si rende necessario uno strutturale potenziamento dell'attuale rete di connessione tra le strutture sanitarie (anche con investimenti regionali) sia dal punto di vista della banda (maggiore velocità) che tal punto di vista della robustezza (continuità di servizio).

Le Aziende sanitarie hanno chiare e documentate esigenze di sicurezza superiori alla norma (materiale riservato, servizi critici, dati sensibili e ultrasensibili), pertanto è raccomandato l'utilizzo di filtri stringenti che blocchino l'uso di strumenti comuni **solo ed esclusivamente** a quei dipendenti e quei sistemi che hanno accesso a questo tipo di informazioni, ed a fronte di forti politiche di sicurezza che istruiscano i dipendenti su come individuare e trattare informazioni riservate, sui pericoli del *phishing*, l'utilizzo di chiavette USB, ecc. ed a fronte della configurazione di strumenti di logging e auditing per mantenere la rete sicura.

Le iniziative condotte a livello regionale per determinare la compliance con il nuovo regolamento GDPR vanno proprio interpretate come modalità di applicazione delle azioni appena descritte.

Alla luce delle priorità indicate in premessa, si dispone che le aziende sanitarie e ospedaliere, nell'ambito della gestione dei sistemi informativi aziendali, applichino i principi contenuti nel presente documento e si adoperino affinché tutte le attività connesse allo sviluppo, manutenzione, evoluzione, conduzione di sistemi informativi siano espletate in completa coerenza con gli stessi.

1. Predisporre le gare di acquisizione di nuovi sistemi informativi o parti di essi avendo come obbligo la proprietà del codice sorgente, che diventa asset strategico aziendale;

2. Promuovere il riuso di soluzioni esistenti, con la diffusione soprattutto delle best practices a livello regionale;
3. Determinare un'effettiva indipendenza dai fornitori di tecnologie, prediligendo soluzione di "open", sviluppate con tecnologie non proprietarie e basate su protocolli ormai diventati standard di fatto nel mondo e-health;
4. Favorire l'interoperabilità e l'integrazione tra sistemi.

7. La carta dei principi tecnologici del procurement[5]

La carta dei principi tecnologici del procurement definisce i criteri minimi per lo sviluppo di servizi digitali della Pubblica Amministrazione che:

- soddisfino le esigenze degli utenti/cittadini;
- siano facilmente manutenibili;
- siano capaci di evolvere in base alle esigenze dei cittadini e al progresso tecnologico;
- siano indipendenti da singole componenti architetturali di terze parti;
- riducano le situazioni di dipendenza da un ristretto numero di fornitori (lock-in).

La carta dei principi tecnologici del procurement raccoglie ed estende le linee guida definite dal Codice dell'Amministrazione Digitale e dal Piano Triennale, riportando in alcuni casi anche norme di legge esistenti, per fornire una visione organica dei principi che la Pubblica Amministrazione e i suoi fornitori dovrebbero rispettare per lo sviluppo di nuovi servizi digitali e per la gestione del ciclo di vita di tali servizi.
Partire sempre dalle esigenze degli utenti. Inserire nel capitolato di gara una specifica richiesta per seguire le linee guida di design e i processi di sviluppo di Designers Italia nella realizzazione dei servizi, seguendo un percorso di User Research, Service Design, User Interface Design e Content Design. Se ritenuto opportuno la fase di User Research può essere condotta anche in via preliminare dalle amministrazioni al fine di supportare la stesura della gara.
Organizzare la progettazione e lo sviluppo dei servizi digitali adottando ove possibile processi incrementali per il rilascio, sfruttando interazioni brevi e frequenti. Il primo rilascio del servizio deve prevedere il numero minimo di funzionalità essenziali utili a raccogliere informazioni dagli utilizzatori e aggiustare il tiro delle fasi successive, che devono essere opportunamente pianificate in durata e numero tali da ottenere una roadmap con rilasci periodici. Ogni rilascio deve essere stato testato da utenti reali e documentato. I capitolati di gara devono prevedere l'applicazione di tale principio.
Assicurarsi che la tecnologia e i servizi sviluppati siano accessibili agli utenti. Inserire nel capitolato l'obbligo di usare gli strumenti forniti da Designers Italia per assicurare che i servizi siano progettati a misura di cittadino, applicando criteri di usabilità e inclusività per aiutare le persone con disabilità.
Pubblicare il codice con licenze open source per migliorare la trasparenza, la flessibilità e la responsabilità: seguire le linee guida per l'acquisizione e il riuso del software. Inserire nel

[5] https://media.readthedocs.org/pdf/carta-dei-principi-tecnologici-del-procurement/latest/carta-dei-principi-tecnologici-del-procurement.pdf

capitolato l'obbligo di rilasciare alla pubblica amministrazione la proprietà intellettuale del software che viene sviluppato ad hoc, incluse le pagine dei siti web, e di pubblicare il software sotto licenza aperta, registrandolo su Developers Italia con i processi indicati nelle linee guida.
Usare standard aperti per garantire che la tecnologia sviluppata funzioni e comunichi con altre tecnologie e possa essere facilmente aggiornata e ampliata. Inserire nel capitolato l'obbligo di utilizzare standard e formati aperti per file e protocolli di comunicazione, l'obbligo di implementare le funzionalità in forma di API documentate secondo le linee guida di interoperabilità, l'obbligo di fornire funzionalità di esportazione di tutti i dati in formati aperti, l'obbligo di documentare la futura procedura di migrazione verso un prodotto alternativo.
Cloud First. Utilizzare sempre prima le risorse del Cloud della PA come indicato dal Piano Triennale in materia di cloud. Inserire nel capitolato l'obbligo di utilizzare le risorse qualificate nell'ambito del Cloud della PA, prediligendo i servizi SaaS dei fornitori qualificati, ogni qualvolta viene sviluppato un nuovo servizio. Qualora i servizi SaaS esistenti nell'ambito del Cloud della PA non siano rispondenti alle esigenze del progetto, prevedere l'utilizzo di servizi infrastrutturali IaaS e PaaS del Cloud della PA; inserire nel capitolato l'obbligo di supporto per il protocollo di rete IPv6.
Mantenere sistemi e dati al sicuro rispettando i livelli minimi di sicurezza. Inserire nel capitolato l'obbligo di rispettare le Misure Minime di Sicurezza, così come previsto dalle linee guida di sicurezza del Piano Triennale; inserire nel contratto clausole di manutenzione che impegnino il fornitore a rilasciare patch di sicurezza che verranno scoperte anche al termine del contratto.
Assicurarsi che i diritti dei cittadini siano protetti integrando la privacy come parte essenziale del sistema. Inserire nel capitolato l'obbligo di rispettare le prescrizioni della normativa italiana ed europea sulla protezione dei dati personali (GDPR).
Promuovere buone pratiche ed evitare duplicazione di sforzi condividendo e riutilizzando servizi, dati e componenti software. Inserire nel capitolato l'obbligo di integrare le piattaforme abilitanti come SPID, pagoPA e ANPR, incluse le piattaforme condivise tipiche del dominio nel quale si opera, come ad esempio il Fascicolo Sanitario Elettronico (FSE), nel caso di una PA dell'ecosistema sanitario; inserire nel capitolato l'obbligo di riutilizzare software, servizi e API messi a disposizione da altre PA evitando ove possibile di re-implementare funzionalità che sono già state implementate da altri; nell'eventualità di sviluppo di nuovi servizi, richiedere che l'applicativo sia sviluppato tenendo presente che possa essere utilizzato da altre PA.
La tecnologia sviluppata o acquistata deve funzionare con il resto delle tecnologie, i processi e le infrastrutture esistenti nell'organizzazione e deve poter adattarsi alle esigenze future. Eseguire una valutazione del debito tecnologico[6] presente nell'organizzazione e pianificare la sostituzione delle tecnologie ormai obsolete per le quali il costo di manutenzione eccede il costo di sostituzione; inserire nel capitolato l'obbligo di utilizzare tecnologie aperte affermate sul mercato e supportate dalla presenza di un'ampia comunità di sviluppatori e utilizzatori;
Studiare e implementare soluzioni per minimizzare la raccolta e facilitare il riutilizzo dei dati evitando la duplicazione di dati. Inserire nel capitolato l'obbligo di utilizzare i dataset rilasciati in open data da altre PA, l'obbligo di utilizzare i vocabolari controllati e le ontologie descritti nel

[6] Per debito tecnologico si intende la sommatoria di tutte le inefficienze dovute a processi duplicati e lavoro superfluo causato all'interno di un processo da parte dell'infrastruttura tecnologica perché obsoleta o inadeguata.

Piano Triennale, l'obbligo di rilasciare in open data tutti i dati prodotti dagli applicativi per i quali la pubblicazione non sia esplicitamente vietata per legge.
Ridisegnare i processi automatizzando il lavoro ripetitivo. È necessario ridisegnare e ripensare i processi rendendoli nativamente digitali, ridurre il più possibile l'intervento manuale nelle attività ricorrenti e non qualificate (data entry, etc.), automatizzando i processi necessari all'erogazione di un servizio e utilizzando l'intervento umano per il controllo della qualità e il monitoraggio.
Stabilire i livelli di servizio per i servizi erogati. Utilizzare indicatori (SLI, Service Level Indicator) oggettivi e misurabili al fine di stabilire obiettivi specifici (SLO, Service Level Objectives) di affidabilità e qualità del servizio, definendo le necessarie penali in caso di mancato raggiungimento degli obiettivi (SLA, Service Level Agreement).
Definire le competenze e i profili necessari per lo sviluppo dei servizi digitali. Valorizzare le professionalità a disposizione della PA seguendo le linee guida per la qualità delle competenze digitali nelle professionalità ICT.
Introdurre sistemi di valutazione dei progetti ex-post. Nelle clausole dei contratti è necessario prevedere sistemi di valutazione dei progetti eseguiti così che le PA possano indirizzare le proprie scelte, anche tenendo conto delle recensioni di altre PA sull'operato di uno specifico fornitore.
Pubblicare i documenti di postmortem quando si verifica un disservizio evidenziando le cause principali e le attività intraprese per evitare che riaccada. Incidenti ed errori sono all'ordine del giorno in ambito tecnologico ed è necessario apprendere da essi per evitare che accadano nuovamente in futuro. Nei contratti con i fornitori è necessario prevedere l'obbligo di fornire una comunicazione puntuale e trasparente delle cause che hanno procurato il disservizio producendo dei documenti di "postmortem" di dettaglio che potranno essere pubblicati dalle amministrazioni.

8. Riferimenti tecnici, amministrativi e linee guida nazionali

Di seguito sono elencate le principali linee guida prodotte da AgID e Team per la trasformazione digitale che devono condurre la progettazione, lo sviluppo, l'implementazione, la gestione e la conduzione dei sistemi informativi delle pubbliche amministrazioni e che devono essere adottate dalle Aziende Sanitarie Locali e dalle Aziende Ospedaliere nella stesura dei documenti tecnici alla base della realizzazione dei sistemi informativi sanitari aziendali.

Obiettivi Piano Triennale

- la condivisione di indicazioni e componenti software che permettano di ridurre i costi di implementazione di nuovi prodotti digitali, favorendo il riuso e l'interoperabilità;
- la diffusione del paradigma open source, agevolando la costituzione di una community di sviluppatori di applicazioni e componenti software di utilità per la PA.

Indicazioni sulle Piattaforme abilitanti e sui progetti strategici

- SPID
- PagoPA
- Fatturazione elettronica
- SIOPE+

Indicazioni sul Modello di interoperabilità

- Linee guida per transitare al nuovo Modello di interoperabilità

Indicazioni sulla Sicurezza

- Linee guida per lo sviluppo in sicurezza del software applicativo

Indicazioni sulla conservazione dei documenti informatici

- Acquisto di servizi utilizzando le gare Consip;
- Accordi di collaborazione tra amministrazioni per la condivisione di infrastrutture comuni dedicate alla conservazione;
- adesione ai servizi offerti dai poli di conservazione.

Principi per lo sviluppo di progetti digitali

- Linee guida di design per i servizi digitali della PA

Standard HL7

Allegati al presente documento:

“ALLEGATO 1 – SINFONIA”

“ALLEGATO 2 – FASCICOLO SANITARIO ELETTRONICO”

REGIONE CAMPANIA – LINEE DI INDIRIZZO PER L'IMPLEMENTAZIONE DEL SISTEMA INFORMATIVO SANITARIO REGIONALE

Allegato 1A

Sinfonia - Architettura Generale del sistema applicativo

Versione 1.00

21 Settembre 2018

SOMMARIO

1. Introduzione

Il presente documento fornisce una panoramica generale dell'organizzazione delle componenti software che compongono il sistema Sinfonia, riportando le diverse "viste" architetturali, che descrivono differenti aspetti del sistema. Esso formalizza le diverse decisioni architetturali e progettuali che sono state prese per le componenti del sistema in oggetto.

2. Scopo e Ambito di Applicazione

Il documento è il risultato delle activity del workflow di Analysis & Design previste dalla metodologia adottata e costituisce l'input per quelle relative al workflow di Implementation & Test; pertanto è destinato a tutti i ruoli coinvolti nelle attività relative a quest'ultimo workflow.

Vengono riportati gli obiettivi ed i vincoli che possono risultare significativi per le restanti viste architetturali (dei Casi d'Uso e Logica).

3. Riferimenti

- Progetto Esecutivo per So.Re.Sa. S.p.A. Società Regionale per la Sanità Regione Campania Rif. Consip ID SIGEF 1607.
- Decreto Dirigenziale n. 131 del 20.06.2018.

4. Termini e definizioni

Modello	Rappresentazione concettuale del sistema ottenuta attraverso l'utilizzo di costrutti linguistici e semantici propri di un linguaggio standardizzato di modellazione (UML).
Package	Elemento del modello che rappresenta un contenitore di altri elementi quali classi, componenti, interfacce, diagrammi, package, ecc.
Componente o Area applicativa	Componente intesa come sistema applicativo oggetto di fornitura o di terze parti.
WEB Tier	Livello architetturale del sistema software dedicato alla interazione con l'utente attraverso tecnologia e protocolli Internet.
EJB Tier	Livello architetturale del sistema costituito da tutti i componenti software relativi all'area della logica applicativa (Business Rules).
Documento HTML	Un documento HTML è un documento SGML che soddisfa i requisiti delle specifiche W3C.
J2EE (Java 2 Enterprise Edition)	Versione enterprise della piattaforma Java.
DAO (Data Access Object)	Pattern che ha lo scopo di disaccoppiare la logica di business dalla logica di accesso ai dati.
HTTP (Hyper Text Transfer Protocol)	Protocollo standard di trasferimento di un ipertesto.
MVC (Model-View-Controller)	Pattern architetturale per lo sviluppo di interfacce grafiche di sistemi software.
SOAP (Simple Object Access Protocol)	Specifica per lo scambio di informazioni strutturate nell'implementazione di Web Services in reti di computer. Il formato dei messaggi è l'XML.
SMTP (Simple Mail Transfer Protocol)	Protocollo standard per la trasmissione via internet di e-mail.

HTML(HyperText Markup Language)	Linguaggio usato per descrivere la struttura dei documenti ipertestuali disponibili nel World Wide Web.
XML (eXtensible Markup Language)	Metalinguaggio standardizzato dal World Wide Web Consortium (W3C).
Stylesheet	Lo Stylesheet (foglio di stile) specifica il formato di presentazione di un documento XML descrivendo sia la trasformazione (opzionale) della struttura del documento di ingresso in un'altra struttura sia come devono essere visualizzati gli elementi della struttura. Il linguaggio per definire un o stylesheet è XSL (eXtensible Stylesheet Language).
XHTML (eXtensible HyperText Markup Language)	Versione aggiornata ed estesa dell'HTML.
JVM (Java Virtual Machine)	Macchina virtuale che esegue programmi in linguaggio Java bytecode.
JS (JavaScript)	Linguaggio di scripting.
DB	DataBase.
Certificato Digitale	Documento elettronico che attesta, con una firma digitale di una certification authority riconosciuta, l'associazione tra una chiave pubblica e l'identità di un soggetto. I certificati digitali aderiscono al formato internazionale ITU-T X.509 secondo quanto descritto dallo standard PKIX “Certificate and CRL Profile”.
Certification Authority (CA)	Entità preposta alla creazione, emissione e garanzia dei certificati digitali, cioè crea ed assegna una determinata coppia di chiavi pubblica e privata e garantisce sull’identità del possessore di tale coppia di chiavi. Gli standard di riferimento per la realizzazione della CA sono RFC2510 ed RFC2511. I certificati devono aderire allo standard X.509 v3 con tutte le estensioni previste in RFC3260. Ulteriori requisiti per i certificati sono specificati dalla RFC3039 che definisce la struttura dei Qualified Certificates come specificato nella European Digital Signature Directive. Responsabilità della CA è anche la

	pubblicazione delle Certificate Revocation Lists (CRLs) secondo lo standard X.509 v2 specificato in RFC2459 e RFC3280.
Registration Authority (RA)	Entità dedicata alla registrazione degli utenti e all'accettazione delle richieste per i certificati. Raccoglie le informazioni dell'utente, esegue la verifica della sua identità, che viene quindi utilizzata per la registrazione dello stesso secondo le policy accordate. Gestisce la revoca dei certificati e le Certificate Revocation Lists (CRLs) e comunica con i protocolli ed i formati specificati in RFC2510bis ed RFC2511bis. Inoltre fa da interfaccia verso il Repository che pubblica i certificati emessi dalla CA e le CRLs. La RA è anche preposta alla scrittura delle smartcard quando è richiesta la generazione centralizzata della coppia di chiavi.
RA Repository	Il luogo dove vengono registrati i certificati, le chiavi, le Certificate Revocation Lists (CRLs).
Certificate Revocation List (CRL)	Lista di certificati digitali revocati perché non sono più validi a causa di molteplici ragioni tra cui compromissione della chiave privata, cambio dei dati personali, scadenza. Le CRL aderiscono al formato internazionale ITU-T X.509 secondo quanto descritto dallo standard PKIX "Certificate and CRL Profile".
PKI (Public Key Infrastructure)	Standardizza l'insieme di tecnologie, infrastrutture, e pratiche di management richieste per abilitare e rendere effettivo l'uso di autenticazione, cifratura e firma elettronica basate su chiave pubblica in applicazioni distribuite (Certificati Digitali, Certification Authority (CA), Registration Authority (RA), Repository e Certificate Revocation List (CRL)).
UDDI (Universal Description Discovery and Integration)	Registry (base dati ordinata ed indicizzata), basato su XML ed indipendente dalla piattaforma hardware, che permette alle aziende la pubblicazione dei propri dati e dei servizi (Web services) offerti su internet.

ESB (Enterprise Service Bus)	Un Enterprise Service Bus (ESB) è un'infrastruttura software che fornisce servizi di supporto ad architetture SOA complesse. Un ESB si basa su sistemi disparati, interconnessi con tecnologie eterogenee, e fornisce in maniera consistente servizi di orchestration, sicurezza, messaggistica, routing intelligente e trasformazioni, agendo come una dorsale attraverso la quale viaggiano servizi software e componenti applicativi.
HL7 (Health Level 7)	Health Level 7 (HL7) è un'associazione non profit internazionale che si occupa di gestire standard per la sanità. HL7 è riferito anche ad alcuni degli specifici standard creati da questa associazione (es. HL7 v2.x, v3.0, CDA, ecc.).
Spring	Spring è un framework open source per lo sviluppo di applicazioni su piattaforma Java. A questo framework sono associati tanti altri progetti, che hanno nomi compositi come Spring Boot, Spring Data, String MVC, Spring Batch, eccetera.
Hibernate	Hibernate è una piattaforma middleware open source per lo sviluppo di applicazioni Java che fornisce un servizio di Object-relational mapping (ORM), ovvero gestisce la persistenza dei dati sul database attraverso la rappresentazione e il mantenimento su database relazionale di un sistema di oggetti Java.

5. Vincoli ed obiettivi architetturali

Le soluzioni tecnologiche ed architetturali adottate per la definizione del sistema Soresa rappresentano una evoluzione degli attuali sistemi in essere nel segmento sanitario della Regione Campania. L'architettura applicativa di Sinfonia si arricchisce di tutti gli elementi utili al funzionamento del sistema secondo il paradigma del Cloud e in linea con le soluzioni proposte nella progettazione esecutiva offerta.

Rimane ovviamente la necessità di disporre di applicazioni che sono tra loro interoperabili e che permettono l'effettivo passaggio di informazioni tra gli attori coinvolti senza interruzioni.

L'evoluzione del complesso ecosistema Sinfonia verso un modello di cloud computing introduce una semplificazione architetturale, organizzativa e di cooperazione dei sistemi e rafforza d'altro canto le caratteristiche di affidabilità, scalabilità, disponibilità e sicurezza complessiva del sistema.

L'innovazione architetturale che qui viene presentata è agevolata e trae vantaggio dal nuovo assetto architetturale e tecnologico che si determina con il consolidamento complessivo del sistema in ambiente cloud. Tale riconfigurazione tecnologica centralizzata, favorisce, rispetto all'attuale configurazione architetturale distribuita, l'introduzione di ulteriori componenti middleware standard come più dettagliatamente descritto nel seguito.

Sotto il profilo organizzativo, architetturale e di cooperazione applicativa, rispetto all'attuale modello di dispiegamento, tutte le istanze del sistema gestionale Sinfonia vengono consolidate sul sistema Cloud messo a disposizione da Soresa.

I servizi di Sinfonia sono resi fruibili ad un utente finale tramite applicazioni Web. Il sistema Sinfonia supporta inoltre la cooperazione applicativa con sistemi fruitori mediante l'esposizione di servizi applicativi di cooperazione (in modalità web services e SPCoop).

Le caratteristiche generali della soluzione si basano sugli strumenti tecnici ed architetturali che allo stato attuale appaiono più maturi, stabili e con elevato potenziale di crescita e diffusione. Come accennato, ci si è riferiti ai modelli di comunicazione basata sugli standard nazionali per l'interoperabilità e cooperazione (SPCoop), ai servizi per la sicurezza e la privacy basati su smart card e firma digitale, all'infrastruttura RUPAR-SPC ed ai servizi connessi peraltro già presenti nella Regione Campania.

Elementi fondamentali del modello architetturale sono:

- l'adozione della SOA (Services Oriented Architecture) e dei Web services che forniscono un approccio per la definizione, la pubblicazione e l'utilizzo dei servizi applicativi;
- la Porta di Dominio che costituisce l'interfaccia standard di connessione dei servizi applicativi di ogni dominio alla RUPAR e a SPCoop (Sistema Pubblico di Cooperazione).

L'invocazione dei servizi di cooperazione è basata sulla "Busta e-Gov", per quanto riguarda gli aspetti di sicurezza point-to-point, affidabilità della trasmissione e tracciatura delle comunicazioni e sui linguaggi XML e WSDL, HL7 e sullo standard UDDI per la formalizzazione degli "Accordi di servizio".

L'architettura del sistema proposto si basa sui seguenti standard tecnologici di progetto e sviluppo già in uso:

- adozione di browser Internet standard per la visualizzazione dell'interfaccia utente;
- logica di presentazione web basata sull'impiego di Web Server e pagine dinamiche JSP;
- logica di presentazione di tipo programmatico basata su Web Services con l'utilizzo di XML su protocollo SOAP;
- logica applicativa implementata in architettura J2EE.

Si aggiunge l'uso dei seguenti ulteriori standard:

- Il middleware WSO2 EI (Enterprise Integrator) che include le componenti ESB, MB, BPM e BRM per una architettura orientata ai servizi (SOA).
- JPA/Hibernate per la logica di accesso ai dati.
- Spring per la gestione della logica di presentation.

L'accesso ai servizi offerti dal sistema Sinfonia è realizzato mediante tre differenti modalità:

- utilizzo della logica di Web presentation resa disponibile tramite pagine JSP: modalità fruibile da utenti mediante l'utilizzo di un browser Internet;
- Porta Applicativa: realizza l'esposizione di servizi di cooperazione di Sinfonia secondo la modalità SPCoop a favore di sistemi fruitori cooperanti – di norma – appartenenti a domini organizzativi esterni a quello che ospita Sinfonia;
- Web services: realizza l'esposizione di servizi di cooperazione di Sinfonia a favore di sistemi fruitori cooperanti – di norma – appartenenti allo stesso dominio organizzativo che ospita Sinfonia.

6. Architettura del Software del Sistema Sinfonia

Per ogni istanza Sinfonia il software applicativo è distribuito sui seguenti tier:

- Presentation Tier
- Business Tier

Inoltre il sistema Sinfonia ha la responsabilità dell'esecuzione di elaborazioni batch, cioè di processi la cui esecuzione è asincrona rispetto alla richiesta attivata dall'utente mediante la web application e che non richiedono interazione con l'utente.

6.1. Presentation Tier

Il Presentation Tier del Sinfonia ha la responsabilità di presentare i servizi sia in forma programmatica (Web Services) sia come Web Application per i servizi applicativi e per la generazione di report.

I componenti di questo tier sono:

- Presentation Logic della User Interface
- Presentation Logic dei Web Services
- Report
- HL7 Engine

6.1.1. Presentation Logic della User Interface

La Presentation Logic della User Interface implementa l'interfaccia Web del sistema Sinfonia ed ha la responsabilità della presentazione dei servizi applicativi tramite interfaccia Web (XHTML/HTTP) ad un operatore accreditato tramite una Workstation dotata di internet browser html standard.

La sua implementazione si basa sul Web-tier di un Application Server J2EE compliant, costituito da un Web Server e un Web Servlet Container che costituisce il contenitore standard per i componenti di front end della tecnologia J2EE: Servlet e Java Server Pages (JSP).

Questo componente si occupa del dispatching delle richieste HTTP provenienti dal browser client e provvede alla generazione dinamica delle pagine XHTML di risposta. Ha la responsabilità della uniformità dell'interfaccia grafica, della gestione delpage flow e del mantenimento dello stato conversazionale con il client (sessione).

La generazione dinamica delle pagine XHTML di risposta ed il controllo del flusso delle pagine web generate dinamicamente avviene seguendo il modello definito dal pattern MVC (Model View Controller).

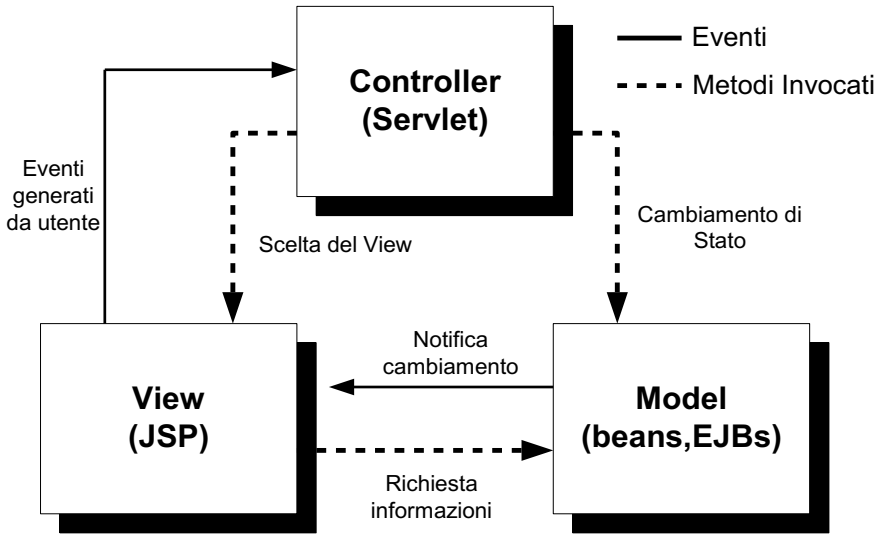

Figura 1 – Il Pattern MVC

In questo modello generale la Servlet (Controller) si comporta da motore web: in base all'input dell'utente, sul quale esegue una verifica di consistenza, decide quale processo di business invocare e seleziona la View successiva.

La View è costituita da una pagina JSP che dinamicamente costruisce il suo contenuto in base ai cambiamenti avvenuti nel Model, vale a dire recupera il risultato della transazione innescata dalla Servlet e lo visualizza formattato all'utente.

Il Model è il sistema contenente la logica di business con cui l'utente interagisce innescando processi atti a conoscerne o alterarne lo stato.

L'uso del pattern MVC permette il completo disaccoppiamento fra la logica di presentation implementata nelle pagine JSP e la logica di controllo implementata nel codice della Servlet.

La specifica implementazione di MVC per i Servizi Applicativi di Sinfonia prevede che:

- il Model renda disponibile il risultato di una transazione lanciata dalla Servlet nell'oggetto HTTPSession (oggetto standard contenente i dati di sessione);
- la JSP raccolga e renda visibile tale risultato all'utente titolare della sessione;

Nell'architettura dei servizi applicativi di Sinfonia il ruolo del Model specificato nel pattern MVC è ricoperto, in linea con quanto dettato dal pattern Business Delegate, da un componente definito EJB Delegate a cui viene delegata la lookup, tramite JNDI, degli EJBs nell'EJB-tier che realizzano il Business Tier, disaccoppiando quindi in maniera completa la logica di controllo e di presentation dalla logica applicativa e di integrazione.

Rientra nella responsabilità della Servlet la gestione della sessione HTTP, ovvero dello stato conversazionale con il client, il controllo di consistenza dei dati inseriti dall'utente nella form e la gestione di situazioni anomale con presentazione all'utente di una pagina di errore. E' previsto l'uso di una Servlet e quindi di uno specifico flusso di pagine per ogni singolo caso d'uso del sistema e le responsabilità della Servlet sono distribuite su più classi di supporto (helper) al fine di rendere più modulare e manutenibile il codice.

I dati manipolati nel Presentation-tier sono modellati da classi di business (Business Object) che rappresentano le entità presenti nel dominio del problema (ad es. assistibile, esenzione ecc.).

Le pagine JSP che prevedono l'immissione dell'input da parte dell'utente (form) fanno uso di codice JavaScript eseguito lato client dal browser per un primo controllo formale sull'input dell'utente al fine di evitare inutile traffico in rete; tale controllo è in ogni caso ripetuto dalla Servlet lato server per verificare comunque l'integrità dei dati ricevuti ed in modo che l'eventuale disabilitazione del supporto JavaScript del browser non sia bloccante per l'applicazione.

0.1.1.1 DAO del Web-tier

Il pattern architetturale DAO qui descritto viene adottato per realizzare l'accesso ai dati nel Web-tier da parte delle componenti di Web presentation.

Tali accessi non sono utilizzati dalla logica di business dell'applicazione ma sono finalizzati esclusivamente al reperimento di informazioni utili per popolare combo box, list box, drop–down list, label, menù etc., quindi informazioni utili alla presentation logic.

6.1.2. Presentation Logic dei Web Services

La Presentation Logic dei Web Services ha la responsabilità della presentazione dei servizi applicativi tramite interfaccia programmatica basata sul web service standard SOAP.

I servizi esposti con tale modalità vengono fruiti da:

- Porta Applicativa della Porta di Dominio per la cooperazione applicativa interdominio standard SPCoop;
- applicativi che non utilizzano SPCoop e che interagiscono con la presentation logic del dominio di riferimento con modalità web service standard SOAP.

La scelta progettuale di utilizzare JAX-WS e JAXB per l'implementazione della Presentation Logic dei Web Services comporta una visione che implica il pensare un web service in termini di RPC basato su SOAP partendo dall'implementazione Java del servizio realizzata tramite POJO (Plain Old Java Object).

Un POJO è una semplice classe Java che non ha un legame diretto con un container o un application server e quindi non implementa interfacce specifiche e non estende classi specifiche. Il POJO contiene metodi che implementano i servizi che vanno esposti sotto forma di web services ed a questo scopo in esso vengono utilizzate le "annotations" (informazioni per il compilatore o per il runtime che non hanno influenza sul codice Java), una caratteristica introdotta nel linguaggio Java a partire da J2SE 5 (1.5).

L'ambiente operativo per l'esecuzione dei POJO e per l'esposizione dei web services è costituito dal framework WSIT (Web Services Interoperability Technology). WSIT è l'implementazione del web services stack Metro, progetto open source supportato da Sun Microsystems prima e da Oracle ora. WSIT implementa gli standard più recenti di SOAP, WSDL e WS-* (con una particolare cura per WS-Security). La principale caratteristica del WSIT (detto anche stack Metro) è la completa aderenza agli standard JSR e JAX-* e la completa e garantita interoperabilità con i Framework Microsoft .NET 3.0 e .NET 3.5.

Lo scheletro di un POJO, con le relative annotazioni necessarie a renderlo un web service viene tipicamente costruito automaticamente dall'IDE che provvede anche alla definizione del relativo WSDL che, all'atto del deploy del servizio, viene pubblicato da una URL specificata. Inoltre l'IDE consente l'aggiunta degli handler per espandere le funzioni infrastrutturali del servizio come ad esempio la gestione trasparente di aspetti come la gestione degli errori (fault), il log e la sicurezza.

L'implementazione dei web services è orientata alla invocazione remota di un metodo Java via SOAP, interoperabile con altre piattaforme che implementano i web services.

Per i dettagli circa identificazione, autenticazione ed autorizzazione si faccia riferimento al paragrafo Identificazione e Autenticazione per i servizi di cooperazione.

Ciascun web service di Sinfonia sarà quindi costituito delle seguenti componenti principali:

- POJO (Plain Old Java Object);
- VO (Value Object).

0.1.1.2 POJO

Per poter esporre un servizio di cooperazione mediante un web service è necessario definire classi Java denominate POJO (Plain Old Java Object), che ne implementano il comportamento. Tali classi di implementazione fanno uso delle *java-annotation* standard, del package *javax.jws.**.

Utilizzando le *java-annotation* il framework di web-services, a run-time, sull'application-server, genera automaticamente per ogni POJO un WSDL.

Sarà realizzata una classe POJO di implementazione per ogni entità.

Ogni metodo della classe POJO implementa una operation del web service, descritta nel WSDL del web service ed esposta sui nodi di Sinfonia. Il nome del metodo deve essere uguale al nome della operation riportato nel documento di architettura dell'area.

0.1.1.3 Value Object (VO)

I metodi dei POJO (come ogni metodo Java) prevedono parametri di input e output.

Ciascun parametro è in alternativa:

- tipo elementare (tipi primitivi e classi standard Java ad es. String e wrapper)
- tipo complesso, realizzati mediante classi denominate Value Object (VO) che contengono soltanto attributi ed i relativi metodi *set* e *get*.

Le classi Value Object saranno collocate in un package e sono costruite a partire dalla definizione dell'input e dell'output di ciascuna operation, secondo quanto specificato nei documenti di architettura di ciascuna area applicativa

6.1.3. Report

Per la realizzazione dei report vengono utilizzate le librerie:

- Java Reporting Component (JRC) Ver. 11.8 o successiva di Business Object per integrare nell'applicazione la generazione dei report;
- Report Designer Crystal Reports 2008 per la fase di design di ogni report.

Le JRC costituiscono un efficace modulo di creazione di report che sfrutta appieno i vantaggi offerti dalla portabilità Java su più sistemi operativi e piattaforme hardware.

0.1.1.4 Integrazione report interattivi

L'integrazione di ogni report all'interno della web application avviene tramite i componenti:

- **Report Engine:** processa la richiesta di report ricevendo l'opportuno file .rpt e rende disponibile il report source risultante al Report Viewer.
- **Report Viewer:** esegue il rendering di un report nel formato di esportazione scelto dall'utente fra PDF e RTF.

La servlet gestisce il caso d'uso di generazione del report raccogliendo i parametri necessari alla generazione del report, gestisce l'eventuale esportazione del report nei formati previsti. Il report generato viene reso visibile all'utente tramite il Report Viewer, il tutto nel pieno rispetto del pattern MVC.

6.1.4. HL7 CDA

Nell'ambito del progetto Sinfonia il trattamento dei dati clinico-sanitari si basa sulla gestione di documenti XML in un tipico approccio document-oriented. La struttura di tali documenti XML è conforme allo standard HL7v3/CDA rev.2 e costituisce il veicolo di trasporto dei dati clinici in documenti (atti sanitari) firmati digitalmente (nel seguito documenti CDA).

CDA (Clinical Document Architecture) è una specifica XML di HL7 riconosciuta dall'ANSI per la rappresentazione standard di dati clinici. HL7 CDA è uno standard diffuso a livello internazionale, di conseguenza, la sintassi e la semantica dei metadati ha una valenza "globale" e la loro implementazione rappresenta un efficace strumento verso l'interoperabilità documentale.

Si rimanda a documenti Specifica dei Requisiti Software delle aree applicative per i tipi di CDA trattati.

6.2. Business Tier

Il Business Tier del sistema Sinfonia è responsabile della realizzazione della logica di business.

L'implementazione di questo strato si basa sull'EJB-tier di un Application Server J2EE compliant, contenente l'EJB Container che costituisce l'ambiente operativo dei componenti della logica di business nella tecnologia J2EE, gli Enterprise Java Beans (EJB).

L'EJB-tier prevede un doppio strato di EJB:

- lo strato di EJB di facciata, organizzati per entità di business, che espongono metodi in corrispondenza uno a uno con la corrispondente richiesta proveniente dal Presentation Tier;
- lo strato di EJB locali (non visibili all'esterno dell'EJB-container) che espongono, ad uso esclusivo degli EJB di facciata, servizi (transazionali o di accesso ai dati in lettura) organizzati per entità di business.

Lo strato di EJB locali si avvale dei servizi di classi helper che provvedono alla implementazione di controlli formali e applicativi ed alla implementazione di trasformazioni o conversioni di formato.

L'accesso al database dedicato da parte degli EJB avviene tramite il componente DAO (Data Access Object) che viene strutturato in modo che visto dagli EJB locali esporrà un suo sottotipo per ogni business entity. Ognuno di tali sottotipi implementerà le interfacce contenenti gli statement elementari relativi ad ogni singola relational table di cui utilizza i dati per i propri scopi. La transazionalità degli accessi al database sarà gestita dal container degli EJB.

Si sceglie di usare Session EJB di tipo Stateless per due ragioni:

- le richieste provenienti dal Presentation Tier sono di tipo stateless;
- gli Stateless Session EJB sono più efficienti e performanti.

6.3. Elaborazioni Batch

Per elaborazione batch si intende un qualsiasi processo la cui esecuzione è asincrona rispetto alla richiesta attivata dall'utente mediante la web application e che durante la sua esecuzione non richieda interazione con l'utente. Pertanto non necessita di un ambiente operativo J2EE essendo sufficiente l'utilizzo di una JVM.

I casi d'uso che prevedono tali elaborazioni consentono all'utente, tramite interfaccia web, di richiedere una elaborazione batch consentendogli di esplicitare, se necessario, gli opportuni parametri di input. Successivamente un operatore di back office analizza le richieste pervenute e avvia l'esecuzione del processo batch. A processo concluso viene memorizzata su database l'avvenuta esecuzione del processo e l'esito (elaborato con successo o elaborato con errore). Lo stato della elaborazione viene reso disponibile all'utente mediante una funzionalità ad hoc.

L'autorizzazione dell'operatore di back office all'avvio di un processo batch è conseguente alla sua identificazione e autenticazione, mediante username e password, al sistema operativo ed al DBMS.

Dal punto di vista architetturale, le componenti che entrano in gioco nella richiesta e nell'esecuzione del batch sono distribuite su due layer:

- **Presentation Layer** che realizza i casi d'uso di richiesta di elaborazione batch;
- **Business Layer** che contiene la logica di start e di esecuzione del batch, che può essere un processo batch oppure un report batch, cioè un report non interattivo.

6.3.1. Presentation Layer

Il presentation layer è costituito dalle componenti di interfaccia web che consentono all'utente di richiedere l'esecuzione asincrona di un processo batch, fornendo gli opportuni parametri al processo. Tale richiesta, che è a tutti gli effetti un caso d'uso del sistema, viene memorizzata insieme ai parametri di input su database. In un momento successivo la richiesta viene presa in carico da un operatore di back office che avvia il processo batch, ne controlla l'esecuzione, ne analizza l'output e tramite interfaccia web può apporre un flag "visto" alle richieste evase nella tabella delle richieste dove è anche presente un flag di stato che prevede i seguenti valori:

1. "IN ELABORAZIONE" all'atto della richiesta di esecuzione del batch;
2. "ELABORATO CORRETTAMENTE" dopo la corretta esecuzione del batch;
3. "ELABORATO CON ERRORI" se si sono verificati errori nella elaborazione del batch;
4. "ELABORATO CORRETTAMENTE DATI NON TROVATI" se l'elaborazione si è conclusa correttamente ma non sono stati riscontrati dati;
5. "ANNULLATA" quando l'elaborazione viene annullata dall'operatore.

Ciascun processo batch provvede a registrare il proprio cambio di stato e produce un file di log consultabile dall'operatore di back office.

L'operatore che aveva effettuato la richiesta di esecuzione del processo batch può controllarne l'avvenuta esecuzione tramite interfaccia web, e, se previsto, eseguire il download del risultato del processo (report).

Dal punto di vista architetturale il presentation layer è del tutto simile ad un qualsiasi altro caso d'uso. Quindi per i casi d'uso di richiesta elaborazione batch valgono le scelte progettuali e architetturali effettuate per il presentation layer dell'intero sistema.

6.3.2. Business Layer

Il Business Layer delle elaborazioni batch si divide in due categorie diverse sia per il tipo di processo, sia per il risultato prodotto sia per la tecnologia adottata:

- ***Processo Batch***: elaborazione che produce dati che vengono memorizzati sul db;
- ***Report Batch***: elaborazione che produce file report in formato ASCII o pdf.

0.1.1.5 Processo Batch

Un processo batch:

- elabora dati presenti nel database in funzione dei parametri input forniti dall'utente che ha richiesto l'esecuzione del processo batch, anch'essi presenti nel database;
- produce risultati che vengono memorizzati nel database (a titolo esemplificativo rientrano in questa categoria i batch di calcolo delle competenze delle diverse categorie di medici).

Un processo batch è costituito da un programma Java avviato da console, in un momento successivo alla richiesta, da un operatore di back office. E' un processo la cui esecuzione avviene all'interno di una macchina virtuale Java JVM standard J2SE. Per motivi di efficienza, dato il massiccio uso di accessi al database, la JVM di esecuzione può essere quella di una macchina in connessione intranet con Database Server se non una JVM presente sul database server.

0.1.1.6 Report Batch

Un report batch:

- elabora dati presenti nel database;
- l'elaborazione è in funzione dei parametri input forniti dall'utente che ha richiesto l'esecuzione del report batch, anch'essi presenti nel database;
- il layout e la logica di reporting del report sono definiti in un file con estensione .rpt che risiede in un path accessibile dalla macchina in cui risiede la JVM di esecuzione del report batch;
- produce, come risultato della elaborazione un report, cioè un file di dati in formato conforme alle specifiche definite per il report; i dati sono disposti con un layout predefinito in fase di progettazione del report.

Il report batch è costituito da un programma Java avviato da console, in un momento successivo alla richiesta, da un operatore di backoffice, quindi è un processo la cui esecuzione avviene all'interno di una macchina virtuale Java JVM standard J2SE. Per motivi di efficienza, dato il massiccio uso di accessi al database, la JVM di esecuzione può essere quella di una macchina in connessione intranet con Database Server se non una JVM presente sul database server.

Tale programma utilizza le librerie denominate Java Reporting Component Ver. 11.8 (JRC) di Business Object per integrare nell'applicazione la generazione dei report.

Il file con estensione .rpt, che definisce il layout di un particolare report, risiede in un path accessibile dalla macchina in cui risiede la JVM di esecuzione del report batch ed è il prodotto della fase di design del report.

Il design di ogni report viene eseguito con l'ausilio del tool di sviluppo Report Designer Crystal Reports 2008.

7. Componenti per la Firma Digitale

Il processo di firma digitale si basa su PKI (Public Key Infrastructure) che standardizza l'insieme di tecnologie, infrastrutture, e pratiche di management richieste per abilitare e rendere effettivo l'uso di autenticazione, cifratura e firma elettronica basate su chiave pubblica in applicazioni distribuite e garantisce:

- **Autenticazione**, cioè certezza dell'identità di una persona o di un'applicazione
- **Integrità dei dati**, per dimostrare che non vi sono state manipolazioni dei dati durante il trasporto
- **Non ripudio**, per dimostrare l'origine da cui proviene l'informazione.

Oltre all'infrastruttura PKI è necessaria l'emissione, per ogni utente, di una CNS (Carta Nazionale dei Servizi) o token USB.

7.1. CNS, PKCS#11, Wrapper Java, card reader e PC/SC driver

L'interfacciamento fra le applicazioni e la CNS/token è basato sullo standard PKCS#11 implementato tramite librerie software fornite dal produttore della specifica CNS/token utilizzata. Le librerie PKCS#11 comunicano con la CNS tramite una periferica (card reader) collegata ad una porta seriale oppure ad una porta USB del PC, e con i token USB direttamente tramite porta USB. I driver dei card reader vengono forniti dal produttore e sono basati sullo standard PC/SC. Poiché le librerie PKCS#11 sono librerie software a basso livello, la Certification Authority, che tipicamente fornisce sia lettore sia smartcard con credenziali di firma (coppia di chiavi asimmetriche RSA con relativo certificato) conformi alle direttive AIPA, CNIPA, DigitPA e ora AgID fornisce anche librerie che fungono da wrapper per le librerie PKCS#11, implementate con i più diffusi linguaggi di programmazione, incluso Java (come evidenziato in figura).

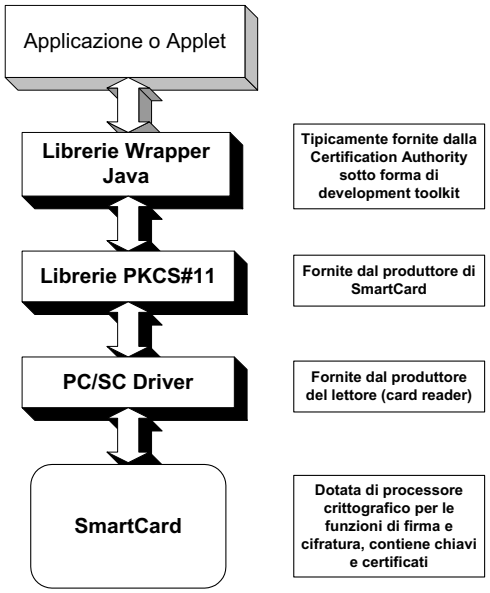

Figura 2 – Gestione CNS

L'eventualità della presenza di più lettori con più CNS inserite viene risolta dallo standard PKCS#11 tramite lo Slot. Lo Slot rappresenta il lettore dal punto di vista logico e pertanto esisteranno tanti slot per quanti lettori di Smartcard vengono rilevati nel sistema.

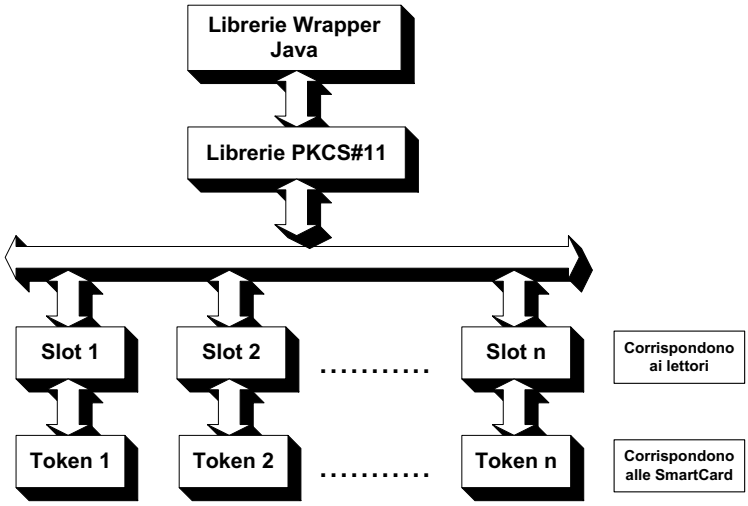

Figura 3 – Gestione di più CNS con Slot

La presenza di una infrastruttura PKI con relativa Certification Authority e di una piattaforma CNS con relativo CardOS, librerie PKCS#11 e Wrapper Java consentono l'implementazione del processo di firma. La fornitura Sinfonia supporta CNS con certificati di autenticazione e di firma rilasciati da CA inserite nel registro dell'AgID.

7.2. Formato dei documenti prodotti e standard di firma

I documenti prodotti da Sinfonia da sottoporre al processo di firma sono dei seguenti formati:

- CDA HL7 come, ad esempio, prescrizioni, erogazioni e referti;
- PDF per qualsiasi altro tipo di documento per cui è necessaria l'apposizione della firma.

E' prevista l'adozione dei seguenti standard di firma riconosciuti con validità legale dal AgID (ex DigitPA e ex CNIPA):

- p7m per il formato HL7 CDA;
- PDF Signature secondo gli standard Adobe Systems Inc. approvati dal AgID (ex DigitPA e ex CNIPA).

Nei documenti SRS di ogni area applicativa verrà inserito l'elenco dei documenti soggetti a firma, il loro formato e la tipologia di firma.

7.3. Controlli di validità su un documento firmato

I controlli effettuati lato server su un documento firmato sono:

a) integrità del documento firmato;

b) validità della firma apposta tramite un certificato digitale X.509v3;

c) integrità e validità del certificato di firma dell'utente.

La validità del certificato digitale X.509v3 di firma prevede che il certificato:

- sia rilasciato da una CA riconosciuta: verifica che il certificato di root della CA, presente nel certificato X.509v3, sia contenuto nel TrustStore del server;
- sia autentico: verifica della validità della firma apposta sul certificato dalla CA;
- sia temporalmente valido;
- contenga il codice fiscale del titolare della CNS/token all'interno del commonName;
- non sia interdetto all'uso (sospeso o revocato): lo stato interdetto di un certificato è verificato mediante l'analisi della CRL indirizzata dalla URI presente nel certificato digitale X.509v3 stesso.

Nel caso di CRL con validità scaduta, la verifica dello stato di interdizione (certificato sospeso, certificato revocato) è subordinata al parametro di sistema che indica se considerare valida la CRL anche se con validità scaduta.

7.4. Il processo di firma digitale

I documenti SRS delle aree applicative riportano nella descrizione dei casi d'uso, ove applicabile, la esecuzione del processo di firma digitale. I documenti SRS delle aree applicative non riportano il dettaglio del processo di firma digitale che risulta essere descritto nella seguente sezione.

Il processo di firma via web prevede la visualizzazione del documento da firmare e, a seguito della conferma da parte dell'utente, l'apposizione della firma digitale. La responsabilità della visualizzazione del documento è a carico della Servlet di Firma. L'apposizione della firma digitale sul documento è a carico dell'Applet di Firma. La responsabilità dei controlli sul documento firmato è a carico della Servlet di Firma.

Insieme all'applet vengono scaricate dal browser le librerie necessarie alle interazioni con la smartcard e l'applet viene eseguita dalla JVM (Java Virtual Machine) all'interno del browser. Essendo una applet che interagisce con componenti hardware e software installati sulla workstation, l'applet deve essere firmata (signed) affinché venga verificata la provenienza e l'autenticità.

La figura che segue descrive la sequenza delle interazioni tra componenti e attori che "partecipano" a questo processo.

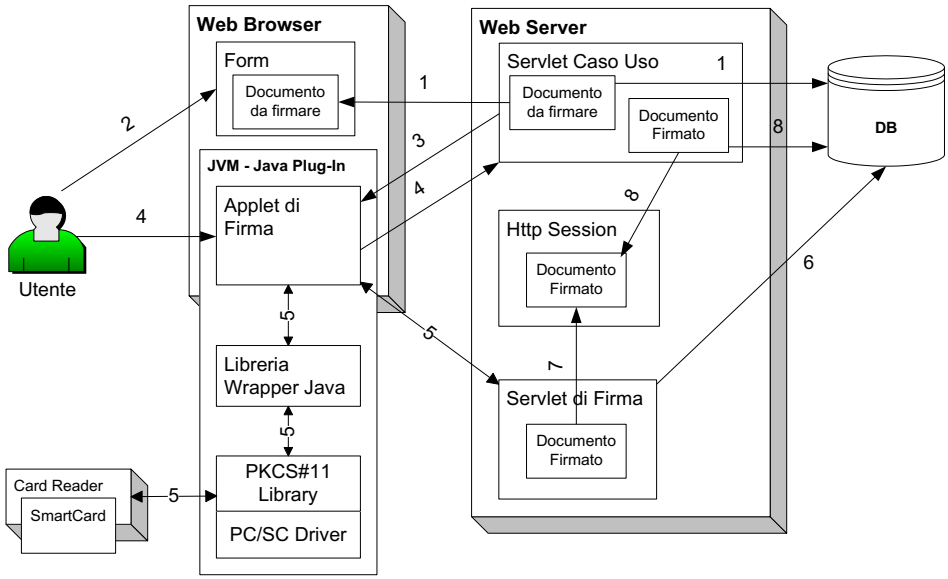

Figura 4 – Processo di Firma

Flusso Principale

1. la Servlet del Caso d'Uso produce il documento conservandone temporaneamente una copia nel DB ed invoca la Servlet di Firma che provvede alla visualizzazione e alla richiesta di conferma;
2. l'utente conferma la volontà di firmare;
3. la Servlet di Firma invia la pagina contenente l'Applet di Firma;
4. l'Applet di Firma scarica il documento dal server, propone – nel caso siano presenti più certificati di firma sulla smartcard - la selezione di uno dei certificati di firma e richiede la digitazione del pin di autenticazione della smartcard e del pin di firma;
5. l'Applet di Firma invoca le funzionalità crittografiche della smartcard, firma il documento e restituisce il documento firmato alla Servlet di Firma;
6. la Servlet di Firma esegue i controlli di validità del certificato di firma e controlla la validità del documento firmato e la sua corrispondenza con il documento da firmare;
7. la Servlet di Firma conserva il documento firmato nel DB;
8. la Servlet del Caso d'Uso recupera il documento firmato dal DB rimuovendo quello temporaneo non firmato.

Flusso Alternativo: *Rifiuto della volontà di firmare*

Se l'utente NON conferma la volontà di firmare il documento, il controllo ritorna Servlet del Caso d'Uso. Il documento non viene né firmato né archiviato. La Servlet del Caso d'Uso deve rimuovere il documento da firmare temporaneamente conservato nel DB.

Flusso Eccezionale: ***Errore di inserimento del PIN***

Se l'utente digita un pin errato, l'Applet di Firma visualizza un messaggio di pin errato. Alla terza digitazione consecutiva di pin errato l'Applet di Firma visualizza un messaggio dove si comunica all'utente che la smartcard è inservibile.

Flusso Eccezionale: ***Esito negativo della verifica di firma.***

La Servlet di Firma invalida la firma se

a) non sono superati i controlli di validità del certificato di firma;

b) non sono superati i controlli di validità del documento firmato;

c) il documento firmato non è identico a quello conservato temporaneamente nel DB prima dell'inizio del processo di firma.

La Servlet di Firma informa dell'esito negativo di verifica di validità della firma.

8. Gestione Utenti, Identificazione, Autenticazione ed Autorizzazione

Il sistema consente di accedere a tutti i servizi offerti, con meccanismi di autenticazione basati su username / password o smart card crittografiche (CIE, CNS, CRS, etc.). Il sistema gestisce, con un'interfaccia, la gestione applicativa di ruoli e profili, che sarà possibile scegliere in fase di accesso. Gli utenti delle singole applicazioni presenti nella fornitura Sinfonia accedono al sistema tramite un unico Front-End Web, la cui implementazione e autenticazione viene demandata al WSO2 Identity Server che interagisce in maniera federata con il Single-Sign On (SSO) regionale. Si rimanda a tale paragrafo per ulteriori approfondimenti in merito.

8.1. Identificazione, autenticazione ed autorizzazione degli utenti

L'identificazione, l'autenticazione e l'autorizzazione costituiscono i passi del processo attraverso il quale una entità accerta la corretta, o presunta, identità digitale di un utente.

Tutte le componenti applicative della fornitura Sinfonia per la fase di identificazione e autenticazione si integrano con il sistema di SSO.

La componente *Gestione Utenti*, invece, fornisce i servizi di amministrazione necessari a definire e profilare utenti nonché i servizi per l'autorizzazione dell'utente all'utilizzo delle singole funzionalità/servizi e alla visibilità di dati sensibili. La componente inoltre ha la responsabilità di produrre la reportistica analitica e riepilogativa relativa all'utilizzo dei servizi, all'assegnazione dei ruoli ed alla distribuzione degli utenti rispetto a ruoli e aziende sanitarie.

8.1.1. Definizione e Profilazione degli Utenti

La definizione e la profilazione di un utente è basata sulla sua identità e sui ruoli, detti Ruoli Istituzionali, che l'utente può assumere all'interno di una o più strutture.

La funzionalità di definizione e profilazione dell'utente fornisce la possibilità, ad un operatore autorizzato tramite interfaccia web, di definire o modificare più corrispondenze fra identità dell'utente, Ruolo Istituzionale e struttura in cui quel ruolo viene ricoperto.

La definizione e profilazione dell'utente in questi termini pone le basi per il processo di autorizzazione basata su ruolo e rende il meccanismo utilizzabile sia nel contesto Regionale che nel contesto aziendale.

8.1.2. Autorizzazione

Il processo di definizione delle autorizzazioni è fondato sui Ruoli Istituzionali e alla attribuzione a ciascun Ruolo Istituzionale di uno o più Ruoli Operativi. Un Ruolo Operativo viene definito come raggruppamento logicamente coerente di servizi ed è gestito solo a livello di backoffice.

Il sistema autorizzerà l'utente alla fruizione di un servizio solo se tale servizio è associato al Ruolo Operativo attribuito al Ruolo Istituzionale ricoperto dall'utente stesso (assegnato nella fase di definizione e profilazione).

Si rimanda alla documentazione delle diverse aree applicative per la semplificazione del modello dei ruoli attualmente previsto.

A livello di backoffice sarà possibile definire o modificare, tramite interfaccia web, il mapping Ruoli Istituzionali – Ruoli Operativi, eliminare un Ruolo Istituzionale, creare un nuovo Ruolo

Istituzionale ed associargli uno o più Ruoli Operativi. I Ruoli Operativi sono predefiniti nel sistema in quanto, per loro stessa natura, legati ai servizi che il sistema offre.

9. Identificazione ed Autenticazione per i servizi di cooperazione

Obiettivo del capitolo è quello di illustrare i meccanismi e le specifiche con cui il sistema Sinfonia implementa i meccanismi di identificazione, autenticazione ed autorizzazione dei sistemi applicativi cooperanti che inoltrano richieste di servizio in modalità web services e in modalità SPCoop.

Nel seguito si intende per Sistema Fruitore un sistema applicativo che fruisce dei servizi di cooperazione di Sinfonia, che funge da Sistema Erogatore. Vengono considerati sistemi fruitori, alla stregua di qualunque altro sistema applicativo cooperante, le stesse componenti applicative ed i sistemi infrastrutturali di Sinfonia per le richieste di servizio che questi inoltrano verso le altre componenti applicative di Sinfonia.

L'identificazione, l'autenticazione e l'autorizzazione del Sistema Fruitore, per ciascun servizio di cooperazione esposto, sono implementati dall'ESB di WSO2.

9.1. Il processo complessivo

Di seguito è illustrato il processo complessivo di interazione tra sistemi cooperanti relativi al processo di identificazione, autenticazione e autorizzazione nel caso di invocazione dei servizi esposti dal Sistema Erogatore Sinfonia attraverso ESB:

1. Il middleware ESB, attraverso proxy service, riceve un messaggio SOAP contenente il certificato X.509v3 del Sistema Fruitore in conformità alla specifica "X.509 Certificate Token Profile" fornito da WS-Security. L'integrità del messaggio è garantita dalla firma digitale apposta con certificato X.509v3.
2. Il middleware ESB verifica l'integrità sintattica del messaggio verificando la rispondenza all'xsd. In particolare viene estratto dal messaggio di input il token X.509v3, rappresentante il Sistema Fruitore. Successivamente si applicano tutti i controlli necessari a verificare la validità del certificato. Ottenuta la validazione del certificato, il middleware ESB accerta la validità dell'identità del Sistema Fruitore interfacciandosi con i servizi esposti dalla propria IdP. In particolare il middleware ESB verifica che il common-name del certificato X.509v3 sia presente ed abilitato nell'Anagrafe dei Sistemi Fruitori autorizzati ad interagire con il Sistema Erogatore.
3. Il middleware ESB, superati tutti i controlli del passo precedente, provvede a reinoltrare la request verso il Sistema Erogatore aggiungendo il CN dell'integratore negli attributiAutorizzativi e inserendo una propria security.
4. Il Sistema Erogatore riceve il messaggio SOAP contenente il certificato X.509v3 del middleware ESB in conformità alla specifica "X.509 Certificate Token Profile" fornito da WS-Security. L'integrità del messaggio è garantita dalla firma digitale apposta con certificato X.509v3.

5. Il Sistema Erogatore verifica l'integrità sintattica del messaggio verificando la rispondenza all'xsd. In particolare viene estratto dal messaggio di input il token X.509v3, rappresentante il Sistema Fruitore. Successivamente si applicano tutti i controlli necessari a verificare la validità del certificato. Ottenuta la validazione del certificato, il Sistema Erogatore accerta la validità dell'identità del Sistema Fruitore interfacciandosi con i servizi esposti dalla propria Anagrafica Sistemi Fruitori. In particolare il Sistema Erogatore verifica che il common-name del certificato X.509v3 sia presente ed abilitato nell'Anagrafe dei Sistemi Fruitori autorizzati ad interagire con il Sistema Erogatore. In questo caso il middleware figura come Sistema Fruitore.
6. Il Sistema Erogatore, superati tutti i controlli del passo precedente ed in conformità con quanto definito nei successivi paragrafi relativi all'autorizzazione per i servizi di cooperazione, provvede ad erogare il servizio richiesto.
7. Il Sistema Erogatore accerta la conformità della richiesta applicativa rispetto alle eventuali politiche di sicurezza aggiuntive specifiche del servizio applicativo richiesto.
8. Il messaggio SOAP di response inviato al middleware ESB, e poi di conseguenza al Sistema Fruitore soddisferà, analogamente al messaggio SOAP di request, la specifica "X.509 Certificate Token Profile" fornito WS-Security.

9.1.1. Identificazione ed autenticazione dei Sistemi Fruitori

L'identificazione e l'autenticazione del Sistema Fruitore è basata sull'utilizzo del certificato X.509v3 di autenticazione del Sistema Fruitore, secondo lo standard Web Services Security *X.509 Certificate Token Profile* (http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf).

L'identificazione del sistema fruitore deve individuare in modo univoco e certo lo specifico sistema che sta invocando il servizio esposto. Ciò significa che due installazioni distinte di uno stesso prodotto software, anche nello stesso dominio organizzativo ovvero anche sullo stesso sistema server fisico, sono identificate tramite due identità differenti e, quindi, tramite due distinti certificati di autenticazione X.509v3.

Ne consegue che ogni sistema fruitore, sia interdominio che intradominio, deve essere dotato di un certificato X.509v3 il cui commonname deve essere censito nell'anagrafe dei certificati X.509v3 associati ai sistemi fruitori autorizzati ad interagire con il sistema erogatore.

Come da standard WS-Security, il certificato di autenticazione X.509v3 sarà utilizzato per la firma di parti del messaggio SOAP. Nel caso specifico si è scelto di firmare:

- il tag <Timestamp>, previsto nell'header del messaggio SOAP;
- il tag <To>, previsto nell'header del messaggio SOAP;
- il tag <Action>, previsto nell'header del messaggio SOAP;
- il tag <MessageID>, previsto nell'header del messaggio SOAP;
- il tag <ReplyTo>, previsto nell'header del messaggio SOAP;
- il tag <AttributiAutorizzativi>, presente nell'header del messaggio SOAP;
- il tag del contenuto applicativo, primo ed unico figlio del tag <Body>.

9.1.2. Integrità del messaggio

L'integrità del messaggio SOAP associato all'invocazione di un web service assicura che i messaggi non siano intercettati e alterati durante lo scambio fra Sistema Fruitore e Sistema Erogatore.

In Sinfonia è garantita l'integrità delle parti fondamentali del messaggio, sottoponendo a processo di firma:

- il tag <Timestamp>, previsto nell'header del messaggio SOAP;

- il tag <To>, previsto nell'header del messaggio SOAP;

- il tag <Action>, previsto nell'header del messaggio SOAP;

- il tag <MessageID>, previsto nell'header del messaggio SOAP;

- il tag <ReplyTo>, previsto nell'header del messaggio SOAP;

- il tag <AttributiAutorizzativi>, presente nell'header del messaggio SOAP;

- il tag del contenuto applicativo, primo ed unico figlio del tag <Body>.

9.1.3. Non ripudio del messaggio

Il non ripudio di un messaggio trasmesso dal Sistema Fruitore al Sistema Erogatore è garantito dall'autenticazione che una firma è in grado di offrire.

Infatti, l'univocità della firma digitale applicata ad un messaggio impedisce che il proprietario della firma disconosca le informazioni contenute nel messaggio firmato.

In Sinfonia, il non ripudio del messaggio è garantito dall'applicazione della firma digitale da parte del Sistema Fruitore al messaggio SOAP-Request per:

- il tag <Timestamp>, previsto nell'header del messaggio SOAP;

- il tag <To>, previsto nell'header del messaggio SOAP;

- il tag <Action>, previsto nell'header del messaggio SOAP;

- il tag <MessageID>, previsto nell'header del messaggio SOAP;

- il tag <ReplyTo>, previsto nell'header del messaggio SOAP;

- il tag <AttributiAutorizzativi>, presente nell'header del messaggio SOAP;

- il tag del contenuto applicativo, primo ed unico figlio del tag <Body>.

9.1.4. Mantenimento delle informazioni della richiesta di servizio

Allo scopo di mantenere le informazioni relative alla richiesta del servizio, in maniera funzionale a dimostrare a terzi la legittimità dell'operato del sistema Sinfonia, solo per i servizi critici (ad esempio quelli che trattano dati sensibili), saranno memorizzati su una apposita tabella persistente i seguenti dati:

- Nome del servizio (prelevato dagli attributi autorizzativi)
- Codice identità utente (prelevato dagli attributi autorizzativi)
- Ruolo istituzionale (prelevato dagli attributi autorizzativi)

- Data e ora richiesta
- Identificativo del sistema fruitore (CommonName del certificato)
- Messaggio SOAP-Request, comprensivo di Header.

La memorizzazione su questa tabella può essere abilitata/disabilitata in qualsiasi momento dall'amministratore di sistema intervenendo su un flag di abilitazione/disabilitazione definito per ogni servizio.

In considerazione delle ripercussioni che tale scelta può avere sul sistema in termini di occupazione dei volumi e di ulteriore carico transazionale, la definizione dei servizi per i quali saranno mantenute le suddette informazioni sarà effettuata congiuntamente con il committente.

9.1.5. Riservatezza del messaggio

La riservatezza del messaggio SOAP deve garantire che i dati trasmessi non siano alterati durante lo scambio e non siano interpretabili da alcuno con l'eccezione di chi ha il permesso di accedervi.

Lo strumento per garantire la riservatezza del messaggio è l'utilizzo di SSL (Secure Socket Layer), che permette di creare un canale protetto per lo scambio di dati tra due Sistemi.

Tutti i servizi di Sinfonia esposti come web services standard sono fruibili su protocollo SOAP su HTTPS.

9.1.6. Firma dei messaggi di risposta

Per garantire integrità, non ripudio e riservatezza dei messaggi di risposta, nelle SOAP-Response saranno firmati, utilizzando il certificato X509v3 della singola istanza logica di Sinfonia e del middleware ESB i tag:

- <Timestamp>
- il tag <To>, previsto nell'header del messaggio SOAP;
- il tag <Action>, previsto nell'header del messaggio SOAP;
- il tag <MessageID>, previsto nell'header del messaggio SOAP;
- il tag <RelatesTo>, previsto nell'header del messaggio SOAP;
- il tag del contenuto applicativo, primo ed unico figlio del tag <Body>.

9.1.7. Identità dell'utente

L'individuazione dell'identità dell'utente del sistema fruitore è una responsabilità del sistema fruitore. Ciò comporta che:

- il sistema erogatore non dispone dell'elenco delle identità degli utenti finali dei sistemi fruitori;
- il sistema erogatore si fida, cioè prende atto, dell'identificazione, dell'autenticazione dell'utente eseguita dal sistema fruitore e dell'autorizzazione all'invocazione del servizio esposto.

L'identità dell'utente è rappresentata nella richiesta di servizio tramite un identificativo significativo per il sistema fruitore che consenta allo stesso sistema fruitore, in caso di necessità, di risalire all'identità reale dell'utente finale. E' raccomandabile l'utilizzo del codice fiscale.

L'identità dell'utente è presente in ogni richiesta di servizio, negli attributi autorizzativi presenti nell'header del messaggio (tag <IdentificativoUtente>), e deve essere utilizzata dal sistema Sinfonia per fini di tracciamento delle operazioni e, quando necessario, per finalità legate allo specifico servizio applicativo richiesto.

9.1.8. Identificazione ed Autenticazione della Porta di Dominio

L'identificazione e l'autenticazione della Porta di Domino mittente è a carico della componente PDD Scatel 3 allocata sulla Porta di Dominio destinataria del messaggio. I meccanismi sono quelli messi a disposizione dalla stessa PDD Scatel 3.

9.2. Autorizzazione per i servizi di cooperazione.

Ogni invocazione di un servizio applicativo esposto dal sistema erogatore Sinfonia è soggetta ad un processo autorizzativo la cui finalità è verificare che il servizio esposto sia invocabile dall'utente del Sistema Fruitore.

Il processo autorizzativo, sia nel caso intradominio sia nel caso interdominio, per ciascun servizio di cooperazione esposto da Sinfonia, è responsabilità di Sinfonia e non è una responsabilità delle porte di dominio.

Tutti gli attributi autorizzativi necessari al processo di autorizzazione devono essere contenuti nell'header del messaggio SOAP-Request.

Il processo autorizzativo è disaccoppiato dalla logica applicativa che implementa il web service e la anticipa temporalmente verificando il match tra gli attributi autorizzativi e il nome del servizio richiesto. Ciò non toglie che la logica applicativa possa estendere il processo autorizzativo implementando un controllo degli accessi basato sullo specifico contenuto applicativo richiesto e/o su altre politiche di natura meramente applicativa.

Pertanto il processo autorizzativo agisce su diversi livelli al fine di garantire una maggiore granularità delle autorizzazioni sia a livello di singolo utente che di singolo Sistema Fruitore.

9.2.1. Autorizzazione del Sistema Fruitore all'uso di Sinfonia

Il middleware ESB dopo aver autenticato e identificato il Sistema Fruitore verifica che quest'ultimo sia abilitato all'invocazione dei web services esposti dal Sistema Erogatore. Il controllo si sostanzia nel verificare che il Sistema Fruitore oltre ad essere censito nell'Anagrafe Sistemi Fruitori abbia l'abilitazione ad interrogare i web services esposti dal Sistema Erogatore. Tale controllo consente di disabilitare l'erogazione di tutti i web service del Sistema Erogatore ad un determinato Sistema Fruitore che sia già censito nell'Anagrafe Sistemi Fruitori e che abbia un certificato X.509v3 valido.

9.2.2. Autorizzazione del Sistema Fruitore all'uso del servizio

Il Sistema Erogatore, dopo che middleware ESB abbia autenticato, identificato e autorizzato il Sistema Fruitore ad interagire con i web service del Sistema Erogatore, verifica che questo possa accedere allo specifico servizio invocato. Ogni sistema fruitore appartiene ad una classe di sistemi (ad esempio CUP, RIS, LIS etc..) e per ogni classe sono definiti i servizi cui la classe è abilitata mediante un caso d'uso di GUIAA.

In particolare il Sistema Erogatore verificherà che la classe a cui appartiene il Sistema Fruitore sia abilitata al servizio.

9.2.3. Autorizzazione dell'utente del Sistema Fruitore

Tale autorizzazione si avvale di una struttura dati denominata <AttributiAutorizzativi>, presente nell'header del messaggio SOAP, che contiene un gruppo fisso minimo di attributi. La struttura dati <AttributiAutorizzativi> potrà essere estesa per rispondere a nuove necessità quali ad esempio:

- definire ulteriori attributi obbligatori
- definire ulteriori attributi da analizzare durante il processo autorizzativo di specifici servizi esposti.

La struttura <AttributiAutorizzativi>, nella sua forma minima risulta così definita:

<AttributiAutorizzativi>

<IdentificativoServizio/>

<IdentificativoUtente/>

<RuoloIstituzionale/>

</AttributiAutorizzativi>

Ove:

IdentificativoServizio	Nome del servizio invocato.
IdentificativoUtente	Identificatore dell'utente finale la cui attività ha determinato l'invocazione del servizio esposto.
RuoloIstituzionale	Ruolo istituzionale dell'utente finale.

La struttura è firmata con il certificato X.509v3 del sistema fruitore per garantire l'integrità e il non ripudio delle informazioni sulla cui base si attua il processo autorizzativo.

In particolare il processo autorizzativo verifica che il ruolo istituzionale posseduto dall'utente, così come asserito dal sistema fruitore, possa invocare il servizio. In altri termini il Sistema Erogatore verifica che la coppia servizio – ruolo operativo(i) sia abilitata, dove ruolo operativo(i) sia uno dei ruoli operativi definiti a partire dal ruolo istituzionale dichiarato dal Sistema Fruitore. Il processo di risoluzione del ruolo Istituzionale in più ruoli Operativi è a carico del Sistema Erogatore.

L'identità dell'utente finale, così come asserita dal sistema fruitore, non interviene nel processo autorizzativo generale del servizio esposto. L'identità dell'utente è utilizzata, insieme alle informazioni della richiesta di servizio sottomessa, al minimo per scopi di tracciabilità.

L'identità dell'utente finale, così come asserita dal sistema fruitore, potrà tuttavia essere utilizzata per eseguire controlli autorizzativi complementari per uno specifico servizio esposto.

9.3. Riepilogo dei controlli eseguiti ad ogni richiesta di servizio di cooperazione

Il sistema Sinfonia provvederà ad ogni richiesta di servizio di cooperazione a:

- controllare la validità sintattica del messaggio SOAP-Request rispetto allo schema xsd del web service invocato (inclusi tutti i tag xml necessari all'espletamento del processo autorizzativo);
- controllare che la data/ora di creazione del messaggio non sia successiva alla data/ora di sistema (considerando un margine di tolleranza configurabile nella differenza di orario fra client e server);
- controllare che la data/ora di scadenza del messaggio non sia precedente alla data/ora di sistema (considerando una determinata soglia di tolleranza configurabile);
- verificare che siano stati firmati tutti i tag soggetti a firma;
- verificare la validità delle firme apposte;
- controllare che il certificato sia integro;
- controllare che il certificato non sia scaduto;
- controllare che la CA che ha emesso il certificato sia presente nel TrustStore presente sul file system del server;
- verificare che la CRL referenziata dal certificato sia presente sul file system del server;
- verificare che il certificato non sia revocato o sospeso (nel caso di CRL con validità scaduta, la verifica dello stato di interdizione è subordinato al parametro di sistema che indica se considerare valida la CRL anche se con validità scaduta);
- controllare l'identità del sistema fruitore: il commonname del certificato X.509v3 del sistema fruitore deve essere presente nell'anagrafe dei sistemi fruitori;
- controllare che il sistema fruitore sia abilitato all'invocazione di servizi esposti dal sistema erogatore;
- controllare che il sistema fruitore sia autorizzato all'utilizzo del servizio richiesto;
- controllare la presenza delle informazioni minime necessarie per il processo autorizzativo: presenza obbligatoria del tag <AttributiviAutorizzativi>, presenza e valorizzazione dei suoi tag figli;
- controllare che il servizio definito negli attributi autorizzativi sia identico al servizio presente nel Body del messaggio;
- controllare che il ruolo istituzionale definito negli attributi autorizzativi sia autorizzato all'utilizzo del servizio richiesto;
- effettuare gli ulteriori controlli applicativi peculiari del servizio.

10.Sicurezza accesso ai dati su DB

Poiché il database contiene i dati, la sua protezione è un aspetto di centrale importanza. In generale è sempre opportuno adottare ulteriori meccanismi di sicurezza esterni al DB, ma comunque aggiuntivi a quelli tipici del RDBMS. Oracle protegge i dati lì dove vengono conservati, all'interno del database, garantendone la protezione a un livello estremamente elevato. L'RDBMS Oracle offre numerose funzionalità di sicurezza, dall'autenticazione utente alla gestione del privilegio ed al controllo dell'accesso.

10.1. Identificazione, autenticazione ed autorizzazione

Gli utenti accederanno al database per il tramite dell'application server che si connetterà al database mediante un pool di connessioni ed utilizzando una specifica utenza. Pertanto il DBMS si *limiterà* ad identificare ed autenticare l'application server, delegando l'identificazione e l'autenticazione dell'utente ai meccanismi già descritti nel precedente paragrafo. All'RDBMS il rimane il compito di verificare le autorizzazioni (Grant) di accesso ai dati in base al ruolo istituzionale dell'utente. Il database del Sistema Sinfonia gestisce il sistema delle autorizzazioni verificando i privilegi assegnati dal database administrator ai ruoli istituzionali. Quindi, dopo la fase di identificazione ed autenticazione, l'utente può eseguire operazioni su un oggetto del database solo se è stato espressamente autorizzato dall'amministratore. Le autorizzazioni (vale a dire ruoli e privilegi) stabiliscono a quali tipi di dati un utente può accedere e che tipi di operazioni può effettuare su tali oggetti. L'utente può eseguire un'operazione su una risorsa o un oggetto di un database, ad esempio una tabella o una vista, solo se è stato autorizzato a compiere tale operazione dall'amministratore. Senza la concessione esplicita di privilegi, l'utente non può accedere ad alcuna informazione del database. Per garantire la sicurezza e la privacy dei dati, è necessario accordare all'utente solo i privilegi di cui necessita per svolgere le proprie funzioni di lavoro, senza concedergli permessi più ampi. Si tratta del cosiddetto "principio del privilegio minimo". Il database Sinfonia gestisce le autorizzazioni mediante privilegi e ruoli.

Riassumendo, il sistema Sinfonia è provvisto di un doppio sistema di profilazione dell'utente: uno al livello applicativo (solo l'utente autorizzato ad una specifica funzione potrà utilizzare la relativa funzionalità dell'applicazione) e il secondo all'interno del database (pur autorizzato al livello applicativo, vengono accordati all'utente i particolari privilegi sui dati necessari allo svolgimento del suo ruolo). Quindi, qualora un utente del sistema riuscisse anche ad aggirare il sistema di autorizzazione dell'applicativo, non riuscirebbe ad utilizzare le funzionalità in quanto non avrebbe le necessarie autorizzazioni al livello di database. Tale sistema garantisce quindi una profilazione dell'utente robusta a garanzia del principio di necessità nel trattamento dei dati che costituisce la precondizione di qualsiasi Sistema Informativo per la garanzia dei dati personali.

10.2. Cifratura

Alcuni requisiti di legge richiedono particolari misure quando dati personali o identificativi siano abbinati a informazioni di tipo sensibile. Ad esempio, l'accesso al nome dell'assistito in quanto tale può non richiedere particolari precauzioni, ma la combinazione del nome o del dato identificativo con informazioni di tipo sensibile può richiedere ulteriori misure di sicurezza come la crittografia.

I meccanismi di cripting dei dati sensibili al livello fisico nel database difendono da eventuali attacchi alla sicurezza che dovessero sopraggiungere dall'esterno del database stesso (ad es. qualcuno che riuscisse ad accedere direttamente al livello di Sistema Operativo ai datafile del database bypassando tutti i meccanismi di sicurezza messi a disposizione da Oracle).

Per questa eventualità il sistema RDBMS si avvale della feature **"Oracle Transparent Data Encription**" mediante il quale si può implementare in maniera trasparente il processo di cifratura dei dati sensibili direttamente nel motore RDBMS. Tale meccanismo consente di applicare la cifratura in maniera selettiva su specifiche colonne oppure a livello di intero tablespace per proteggere tabelle, indici e altri dati con algoritmi di cifratura robusti (3DES o AES fino a 256 bits) e senza la complessità della gestione di chiavi di cifratura.

Inoltre, anche la cifratura all'interno della Base Dati, se pur un valido meccanismo di sicurezza, non risolve il problema del furto dei supporti contenenti i backup. Per risolvere questo problema, il sistema, mediante la option Oracle Advanced Security, consentirà la cifratura dei backup direttamente sul supporto di salvataggio rendendo indecifrabili le informazioni in essi contenute in caso di accessi fraudolenti ai supporti sui quali vengono salvati i backup.

Il sistema implementerà la cifratura dei canali di comunicazione tra il database server e gli application server mediante gli algoritmi di cifratura (SSL/TSL) messi a disposizione da Oracle così come descritto nel successivo paragrafo 5.6.3 Sicurezza di Rete.

Il sistema implementerà, inoltre, il mascheramento dinamico dei dati sensibili mediante l'utilizzo della feature "Oracle Data Redaction" inclusa nella option Oracle Advanced Security. Sarà possibile creare policy che specificano le condizioni che devono essere soddisfatte prima che i dati vengano mascherati e restituiti all'utente. Durante la definizione di tali policy, si potrà specificare quali colonne mascherare, il tipo di protezione che deve essere applicato (totale, parziale, random ecc.) ed i ruoli istituzionali ai quali il dato viene mascherato.

In alternativa, laddove l'utilizzo della feature "Oracle Data Redaction" non consenta di soddisfare pienamente il requisito funzionale del mascheramento dati, si procederà al mascheramento dinamico dei dati sensibili in maniera applicativa.

10.3. Disaccoppiamento tra dati sensibili e anagrafici

Oltre al tradizionale meccanismo di ruoli e privilegi ed ai meccanismi di cripting dei dati sensibili si è ritenuto opportuno adottare, nella quasi totalità dei casi, anche il meccanismo di disaccoppiamento logico dei dati.

Tale meccanismo è ottenuto disaccoppiando le tabelle contenenti dati sensibili da quelle contenenti dati identificativi e correlandole tra loro mediante l'utilizzo di "codici non parlanti" (con tale terminologia ci si riferisce a codici non esplicativi della semantica del dato o a codici possano ricondurre immediatamente alla semantica del dato) oppure, utilizzando sempre codici non parlanti nei casi in cui i dati identificativi dell'utente e le informazioni sensibili siano contenute nella stessa tabella (es. codice fiscale dell'assistito e i codici esenzione sono contenuti nella stessa tabella, ma questi ultimi sono codificati con una codifica del tutto interna al sistema e non conosciuta dall'operatore). Solo in rare eccezioni, a causa della grossa mole dei dati e dell'elevata attività transazionale correlata, si è deciso di non applicare il disaccoppiamento per non impattare pesantemente sulle performance del sistema e si utilizzano quindi soltanto i meccanismi di ruoli e privilegi e di cripting dei dati.

11. Amministrazione Applicativa

L'area applicativa "Amministrazione Applicativa" si occupa della gestione e valorizzazione dei parametri di configurazione per tutte le aree applicative del sistema. L'area implementa componenti e metodi richiamabili dalle diverse altre aree applicative per la lettura dei valori dei parametri di configurazione. La lettura dei valori dei parametri può avvenire a diversi livelli del software:

- nello strato WEB
- nello strato EJB
- nei batch che girano nella JVM di Oracle

12.Tracciabilità e Monitoraggio

La componente Tracciabilità e Monitoraggio fornisce servizi trasversali a tutte le aree applicative, con l'obiettivo di raccogliere e successivamente analizzare informazioni riguardanti gli utenti che accedono al sistema, i servizi da essi richiesti, data ed ora della richiesta, modalità con cui accedono al sistema e fruiscono dei servizi, l'esito del servizio richiesto.

La componente ha la responsabilità di conservare traccia degli eventi che si verificano nell'ambito dei servizi implementati di Sinfonia. Le informazioni raccolte, opportunamente aggregate ed elaborate, permettono di:

- misurare i carichi di lavoro del sistema;
- monitorare il livello delle prestazioni (per ogni servizio il tempo medio di esecuzione);
- elencare le situazioni anomale;
- produrre rapporti sui servizi erogati relativamente ad aree applicative;
- monitorare le modifiche ai dati del database.

Questa componente non ha responsabilità di monitoraggio sistemistico che viene delegato alle componenti di ambiente e di sistema. Più precisamente il monitoraggio sistemistico, in cui si colloca il monitoraggio tecnico dei malfunzionamenti del software (eccezioni, messaggistica di errore, ecc), è delegato all'attività di tipo sistemistico di monitoraggio e controllo del funzionamento del sistema.

12.1. Ambito del tracciamento

Sono oggetto di tracciamento i seguenti eventi:

- utilizzo del singolo caso d'uso, query, report;
- singola funzione elementare del caso d'uso laddove applicabile, per es. per gli use case di tipo CRUD;
- attraversamento di ciascuna pagina di un caso d'uso, query o report;
- utilizzo del singolo web service sia per web services di consultazione sia di tipo transazionale;
- operazioni di CUD sulle persistenze del sistema.

Relativamente agli use case di consultazione, alle query e ai report si provvederà a tracciare i dati riguardanti i filtri di ricerca/consultazione. Non verrà effettuato alcun tracciamento del risultato.

Per quanto riguarda il tracciamento delle operazioni CUD sulle persistenze, si provvederà a tracciare, per ogni tabella sottoposta ad attività di tracing quanto segue:

- nome della tabella soggetta a tracciamento;
- tipo di operazione (insert, update, delete);

- istanze della tabella prima della modifica oppure in caso di inserimento di un nuovo record l'intera istanza inserita; nel caso di cancellazione l'istanza cancellata;
- istanza successiva alla modifica, nel caso di modifica;
- id dell'utente che ha effettuato la modifica;
- data ed ora della modifica.

12.2. Punti di tracciamento nel software

I punti di tracciamento per use case, query, report e web services sono allocati sul layer web.

12.3. Procedura di tracciamento

La strategia di tracciamento prevede due passi:

1. log su files (sul file system dell'application server) mediante utilizzo della libreria log4J;
2. procedura batch notturna che legge i files, inserisce i record di tracciamento in una apposita tabella del DB ed effettua il backup dei files.

12.4. Persistenza

Tutte le informazioni di tracciamento sono registrate in una apposita tabella del DB. Questa tabella è il punto di raccolta di tutte le informazioni dei canali di tracciamento. Le informazioni di auditing sono memorizzate su un'altra tabella del DB.

12.5. Canali di tracciamento

Per canale di tracciamento si intende il flusso di informazioni riguardanti una componente del sistema.

Data l'organizzazione del sistema Sinfonia in aree applicative, si definisce un canale di tracciamento per ogni area applicativa. Ad un canale di tracciamento corrisponderà uno specifico file che conterrà tutte le informazioni tracciate dal sistema secondo quanto definito dalle regole **Ambito del Tracciamento** e **Record di Tracciamento**. Dunque ogni componente software che contiene punti di tracciamento (ad esempio servlet del caso d'uso o servlethelper del caso d'uso) utilizzerà il canale di tracciamento dell'area applicativa di appartenenza.

12.6. Record di tracciamento

Il singolo record di tracciamento deve contenere, per ogni evento, i seguenti dati:

- il momento esatto in cui si è verificato l'evento (data, ora, minuti e secondi);
- l'identificativo dell'operatore che lo ha generato;
- l'identificativo della sessione http gestito dal web server (jboss) in corso;
- l'identificativo della transazione in corso, determinato dal software applicativo;

- la modalità di autenticazione (forte o debole);
- il nome del caso d'uso, query, report o web service;
- il nome della pagina attraversata;
- il nome dell'operazione (RICERCA, INSERIMENTO, CANCELLAZIONE, MODIFICA, DETTAGLIO);
- il flag inizio esecuzione operazione;
- il flag fine esecuzione operazione;
- il flag esito operazione;
- i valori della richiesta, nel caso di consultazione;
- l'eventuale stack-trace dell'eccezione.

12.7. Procedura di auditing

Il meccanismo di auditing prevede l'attivazione di trigger sul DBMS ad ogni operazione di inserimento, modifica e cancellazione sulle tabelle del DB di interesse. I trigger provvederanno ad inserire i dati definiti nella regola **Record di auditing** in una apposita tabella di auditing. Tali trigger prelevano la UserId dell'utente dalla tabella degli username. La tabella degli username viene valorizzata dalle transazioni applicative attraverso il metodo *pre()* degli EJB di tipo transazionale, invocato prima di ogni transazione. Alla fine della transazione viene poi invocato il metodo *post()* che provvede a cancellare la UserId dalla tabella degli username.

12.8. Record di auditing

Il singolo record di auditing deve contenere, per ogni evento, i seguenti dati:

- il momento esatto in cui si è verificato l'evento (data, ora, minuti e secondi);
- l'identificativo dell'operatore che lo ha generato (UserId);
- il nome della tabella impattata;
- il tipo di operazione (INSERT, UPDATE, DELETE);
- stringa contenente il valore del record prima della modifica;
- stringa contenente il valore del record dopo la modifica.

REGIONE CAMPANIA – LINEE DI INDIRIZZO PER L'IMPLEMENTAZIONE DEL SISTEMA INFORMATIVO SANITARIO REGIONALE

Allegato 1B
Sinfonia - Architettura Generale del sistema applicativo Flussi

Versione 1.00

21 Settembre 2018

Indice dei Contenuti

1. Introduzione

1.1. Generalità

Il presente documento fornisce una panoramica generale dell'architettura di Sinfonia in termini di sistemi e componenti applicative che lo costituiscono e relativa organizzazione strutturale e tecnologica. Il documento definisce:

- gli elementi cardine dell'architettura dei sistemi applicativi oggetto di fornitura, partendo da quanto previsto nel progetto esecutivo;
- gli obiettivi architetturali ai quali si conformano le soluzioni adottate ed oggetto di fornitura;
- i modelli architetturali e i pattern di riferimento per i sistemi e le relative componenti applicative;

Il documento definisce gli obiettivi architetturali del sistema, i sistemi cooperanti, l'architettura tecnologica generale e la distribuzione dei componenti software applicativi ed infrastrutturali sui diversi nodi dell'infrastruttura. Viene inoltre definita l'architettura applicativa di ciascun sistema, mediante specificazione sui diversi layer dei pattern di sviluppo, delle tecnologie e degli standard e meccanismi necessari per assolvere agli obiettivi architetturali.

Esso formalizza le diverse decisioni architetturali e progettuali definite per le componenti preliminarmente alla realizzazione, configurazione ed adeguamento delle stesse ai requisiti di processo e funzionali definiti nel workpackage di "*Analisi e Progettazione*".

1.2. Scopo e Ambito di Applicazione

Il documento è il risultato delle activity del workflow di Analysis & Design previste dalla metodologia adottata e costituisce l'input anche per quelle relative al workflow di Implementation & Test; pertanto è destinato a tutti i ruoli coinvolti nelle attività relative a quest'ultimo workflow.

Definisce principalmente gli aspetti riguardanti la logical view, l'implementaion view e la deployemnt view dell'intero sistema. Tali viste vengono quindi integrate e "complementate" dalle viste dei casi d'uso e dei processi di cui ai documenti di specifica dei requisiti software e di architettura di ciascuna componente applicativa per costituire la "Definizione architetturale" complessiva del sistema Sinfonia.

1.3. Ciclo di vita del documento

Il documento sarà revisionato ed aggiornato a seguito dello svolgimento delle attività di sviluppo delle componenti software qualora vengano rilevati, in fase di definizione di tali artifact ulteriori obiettivi e vincoli architetturali che richiedano la revisione dell'architettura definita da questo documento.

1.4. Riferimenti

1. Progetto Esecutivo per So.Re.Sa. S.p.A. Società Regionale per la Sanità Regione Campania Rif. Consip ID SIGEF 1607.
2. Decreto Dirigenziale n. 131 del 20.06.2018.

1.5. Glossario

Modello	Rappresentazione concettuale del sistema ottenuta attraverso l'utilizzo di costrutti linguistici e semantici propri di un linguaggio standardizzato di modellazione (come ad esempio UML).
Package	Elemento del modello che rappresenta un contenitore di altri elementi quali classi, componenti, interfacce, diagrammi, package, ecc.
Componente (o Area applicativa)	Modulo o sistema applicativo oggetto di fornitura o di terze parti.
WEB Tier	Livello architetturale del sistema software dedicato alla interazione con l'utente attraverso tecnologia e protocolli Internet.
Documento HTML	Documento SGML che soddisfa i requisiti delle specifiche W3C.
Stylesheet	Specifica del formato di presentazione di un documento XML con descrizione della trasformazione (opzionale) della struttura del documento di ingresso in un'altra struttura e della modalità di visualizzazione degli elementi della struttura. Il linguaggio per definire uno stylesheet è XSL (eXtensible Stylesheet Language).

Tabella 1 - Glossario

1.6. Acronimi

JEE (Java Enterprise Edition)	Versione enterprise della piattaforma Java.
DAO (Data Access Object)	Pattern che ha lo scopo di disaccoppiare la logica di business dalla logica di accesso ai dati.
HTTP (Hyper Text Transfer Protocol)	Protocollo standard di trasferimento di un ipertesto.
MVC (Model-View-Controller)	Pattern architetturale per lo sviluppo di interfacce utente dei sistemi software.

SOAP	Specifica per lo scambio di informazioni strutturate nell'implementazione di Web Services in reti di computer. Il formato dei messaggi è l'XML.
HTML(HyperText Markup Language)	Linguaggio usato per descrivere la struttura dei documenti ipertestuali disponibili nel World Wide Web.
JSON (JavaScript Object Notation)	È basato sul linguaggio JavaScript Standard ECMA-262 3ª edizione dicembre 1999, ma ne è indipendente. Viene usato in AJAX come alternativa a XML/XSLT.
XML (eXtensible Markup Language)	Metalinguaggio standardizzato dal World Wide Web Consortium (W3C).
XHTML (eXtensible HyperText Markup Language)	Versione aggiornata ed estesa dell'HTML.
JVM (Java Virtual Machine)	Macchina virtuale che esegue programmi in linguaggio Java bytecode.
DB	Database.
UDDI (Universal Description Discovery and Integration)	Registry (base dati ordinata ed indicizzata), basato su XML ed indipendente dalla piattaforma hardware, che permette alle aziende la pubblicazione dei propri dati e dei servizi (Web services) offerti su internet.
SQL (Structured Query Language)	SQL (Structured Query Language) è un linguaggio standardizzato per database basati sul modello relazionale (RDBMS)
SOA (Service Oriented Architecture)	Architettura software atta a definire l'uso dei servizi per supportare le richieste degli utenti.
SCA (Scalable Cooperative Architecture)	Architettura cooperativa e scalabile
BPM (Business Process Management)	Il Business process management è l'insieme di attività necessarie per definire, ottimizzare, monitorare e integrare i processi aziendali, al fine di creare un processo orientato a rendere efficiente ed efficace il business dell'azienda.
ESB (Enterprise Service Bus)	Un Enterprise Service Bus (ESB) è un'infrastruttura software che fornisce servizi di supporto ad architetture SOA complesse. Un ESB si basa su sistemi disparati, interconnessi con tecnologie eterogenee, e fornisce in maniera consistente servizi di orchestration, sicurezza, messaggistica, routing intelligente e trasformazioni, agendo come una dorsale attraverso la quale viaggiano servizi software

	e componenti applicativi.
JAX-WS (Java API for XML Web Service)	JAX-WS (Java API for XML Web Services) è un insieme di procedure (API) del linguaggio di programmazione Java dedicate allo sviluppo di servizi web. L'insieme fa parte della piattaforma Java EE. Come altre API della Java EE, JAX-WS usa annotazioni, introdotte nella Java SE 5, per semplificare lo sviluppo e implementazioni di client e terminali di servizi web. JAX-WS fa parte del kit di sviluppo Java per web services (Java Web Service Development Pack – JWSDP) e include Java Architecture for XML Binding (JAXB) e SOAP.
JAX-B (Java API for XML Binding)	JAXB è una delle API della Java Enterprise Edition, fa parte del Java Web Services Development Pack (JWSDP) ed è una delle tecnologie di base del progetto Web Services Interoperability Technology (WSIT) promosso dalla Sun Microsystems; inoltre, a partire dalla versione 1.6, JAXB è inclusa anche in Java SE. Java Architecture for XML Binding (JAXB) permette agli sviluppatori Java di effettuare il mapping tra classi e una loro corrispondente rappresentazione XML. JAXB fornisce la possibilità di serializzare oggetti Java in XML (marshalling) e di effettuare l'operazione inversa (unmarshalling), cioè permette di ottenere a partire da un file XML la corrispondente rappresentazione a oggetti Java. JAXB permette quindi di manipolare file XML senza la necessità di implementare alcuna routine specifica per il salvataggio e la lettura di dati. JAXB 1.0 fu sviluppato nell'ambito del Java Community Process come JSR 31. Dal 2006, JAXB 2.0 viene sviluppata come JSR 222. L'implementazione delle specifiche di JAXB è rilasciata sotto licenza CDDL.
WSDL (Web Service Description Language)	Il Web Services Description Language (WSDL) è un linguaggio formale in formato XML utilizzato per la creazione di "documenti" per la descrizione di Web Service.
PEC (Posta Elettronica Certificata)	PEC è l'acronimo di Posta Elettronica Certificata. È un sistema di "trasporto" di documenti informatici del tutto simile alla posta elettronica "tradizionale", cui però sono state aggiunte le caratteristiche per

	garantire agli utenti la certezza, a valore legale, dell'invio e della consegna dei messaggi e-mail al destinatario.
JSP (Java Server Pages)	JavaServer Pages è una tecnologia di programmazione Web in Java per lo sviluppo della logica di presentazione (tipicamente secondo il pattern MVC) di applicazioni Web, fornendo contenuti dinamici in formato HTML o XML. Si basa su un insieme di speciali tag, all'interno di una pagina HTML, con cui possono essere invocate funzioni predefinite sotto forma di codice Java (JSTL) e/o funzioni Javascript. In aggiunta, permette di creare librerie di nuovi tag che estendono l'insieme dei tag standard (JSP Custom Tag Library).
JSTL (Java server pages Standard Tag Library)	JavaServer Pages Standard Tag Library (JSTL) è una libreria inclusa come componente della piattaforma software di sviluppo per applicazioni Web Java EE. È un'estensione di JSP ed incorpora un insieme di tag HTML definiti tramite file XML e programmati in linguaggio Java. Questa libreria è stata rilasciata da società di sviluppo software quali la Sun Microsystems, utilizzabili per la creazione di JavaServer Pages. In alternativa alle librerie di tag standard si possono creare librerie di tag personalizzati, chiamate Custom Tag Library
JPA (Java Persistence API)	Le Java Persistence API, sono un framework per il linguaggio di programmazione Java che si occupa della gestione della persistenza dei dati di un DBMS relazionale nelle applicazioni che usano le piattaforme Java Standard Edition (J2SE) e Java Enterprise Edition (J2EE).
CSS (Cascading Style Sheets)	Il CSS (Cascading Style Sheets, in italiano fogli di stile), in informatica, è un linguaggio usato per definire la formattazione di documenti HTML, XHTML e XML ad esempio i siti web e relative pagine web. Le regole per comporre il CSS sono contenute in un insieme di direttive (Recommendations) emanate a partire dal 1996 dal W3C.
EJB (Enterprise Java Bean)	In informatica gli Enterprise JavaBean (EJB) sono i componenti software che implementano, lato server, la logica di business di un'applicazione web all'interno dell'architettura/piattaforma Java EE espletando servizi a favore della parte di front-end

	ovvero per la logica di presentazione di un'applicazione web. Rappresentano dunque uno strato software residente su un application server all'interno di un'architettura software di tipo multi-tier. Le specifiche per gli EJB definiscono diverse proprietà che questi devono rispettare, tra cui la persistenza, il supporto alle transazioni, la gestione della concorrenza e della sicurezza e l'integrazione con altre tecnologie, come JMS, JNDI, e CORBA. Lo standard attuale, EJB 3, completato nella primavera del 2006, differisce notevolmente dalle versioni precedenti. Gli EJB necessitano di un EJB container tipicamente implementato all'interno degli application server assieme al servlet container per la parte di front-end.
Ajax (Asynchronous JavaScript and Xml)	In informatica AJAX, acronimo di Asynchronous JavaScript and XML, è una tecnica di sviluppo software per la realizzazione di applicazioni web interattive (Rich Internet Application). Lo sviluppo di applicazioni HTML con AJAX si basa su uno scambio di dati in background fra web browser e server, che consente l'aggiornamento dinamico di una pagina web senza esplicito ricaricamento da parte dell'utente. AJAX è asincrono nel senso che i dati extra sono richiesti al server e caricati in background senza interferire con il comportamento della pagina esistente. Normalmente le funzioni richiamate sono scritte con il linguaggio JavaScript. Tuttavia, e a dispetto del nome, l'uso di JavaScript e di XML non è obbligatorio, come non è necessario che le richieste di caricamento debbano essere necessariamente asincrone.
jQuery	jQuery è una libreria di funzioni Javascript per le applicazioni web, che si propone come obiettivo quello di semplificare la manipolazione, la gestione degli eventi e l'animazione delle pagine HTML. È un software liberamente distribuibile e gratuito, come previsto dalla licenza MIT.
JNDI (Java Naming and Directory Interface)	Java Naming and Directory Interface (JNDI) è una API Java per servizi di directory che ricopre un ruolo molto importante all'interno di un application server.

Tabella 2 - Acronimi

2. Vincoli ed obiettivi architetturali

Le soluzioni tecnologiche ed architetturali adottate per la definizione del sistema Sinfonia si basano sulla necessità di disporre di applicazioni che sono tra loro interoperabili e che permettono l'effettivo passaggio di informazioni tra gli attori coinvolti senza interruzioni di processo.

Il sistema informativo Sinfonia è implementato sulla base di uno stile architetturale orientato ai servizi (SOA) ove la cooperazione tra le varie componenti applicative di Sinfonia ed i sistemi esterni avviene attraverso l'esposizione e l'invocazione di servizi SOAP, orchestrati e coordinati attraverso uno strato ESB.

Una istanza del Sistema Applicativo Sinfonia è composta da uno strato applicativo di back end che espone servizi su cui è realizzato uno strato web che rende fruibili ad un utente finale le funzionalità offerte dal sistema. Le caratteristiche generali della soluzione si basano sugli strumenti tecnici ed architetturali che allo stato attuale appaiono più maturi, stabili e con elevato potenziale di crescita e diffusione come i modelli di comunicazione basata sugli standard nazionali per l'interoperabilità e cooperazione, i servizi per la sicurezza e la privacy basati su smart card e firma digitale, PEC.

Elementi fondamentali del modello architetturale sono:

- l'adozione della SOA (Services Oriented Architecture) e dei Web services che forniscono un approccio per la definizione, la pubblicazione e l'utilizzo dei servizi applicativi;
- gli accordi di servizio che specificano gli elementi funzionali e tecnici, necessari per l'invocazione dei servizi;
- lo strato ESB Enterprise Service Bus, che si occupa dell'orchestrazione e della coordinazione dei servizi offerti dalle varie componenti, oltre alle comuni facility previste da un ESB come messaggistica, routing, trasformazione dei servizi, security e single sign on.

Inoltre l'architettura del sistema si basa sui seguenti standard tecnologici di progetto e sviluppo:

- adozione di browser Internet standard per la visualizzazione dell'interfaccia utente dei servizi di back end;
- logica di presentazione web basata sull'impiego di pagine dinamiche (JSP) e delle tecnologie AJAX e JSON;
- logica di presentazione di tipo programmatico basata su Web Services SOAP;
- logica applicativa lato server implementata in architettura JEE, EJB3 e JPA.

L'accesso ai servizi offerti dal sistema Sinfonia è realizzato mediante:

- un sistema di front-end realizzato attraverso un portale che funge da entry point di Sinfonia e permette l'accesso a tutte le componenti applicative;
- un sistema di autenticazione utente di tipo SSO basato su un repository OpenLDAP ed un sistema CAS;
- un insieme di applicazioni web, realizzate mediante tecnologie enterprise come JSP con JSTL, jQuery, Ajax, CSS3 e (X)Html e fruibile dagli utenti mediante l'utilizzo di un browser web;

- un l'Enterprise Service Bus, che si occupa dell'orchestrazione e della coordinazione dei servizi offerti dalle varie componenti, oltre alle comuni facility previste da un ESB come messaggistica, routing, trasformazione dei servizi;
- un registro dei servizi UDDI (service inventory);
- i servizi di cooperazione applicativa, secondo lo standard SOAP, a favore sia di sistemi fruitori cooperanti appartenenti allo stesso dominio organizzativo che ospita il sistema informativo Sinfonia ma anche verso sistemi esterni.

Il modello adottato, fondato sui principi della cooperazione applicativa fra sistemi informativi eterogenei e sul concetto di dominio, prevede l'interconnessione di Sinfonia con lo strato ESB, allo scopo di abilitare l'accesso a tutti gli operatori sanitari della Regione e, in prospettiva, anche agli altri Enti.

La comunicazione tra i vari domini può essere mediata dalle Porte di Dominio, elemento di accesso standard alle risorse applicative dei domini interconnessi, capace di veicolare le richieste di servizio verso altri domini e, simmetricamente, di ricevere le richieste di servizio provenienti dagli altri domini. La sua capacità di interazione con il mondo esterno si fonda sulla comunicazione e sullo scambio di messaggi in formato XML su protocollo SOAP conforme alla Busta di e-government.

2.1. Obiettivi architetturali

Nel presente paragrafo vengono riportati gli obiettivi architetturali che saranno soddisfatti dal presente documento.

Denominazione	**Descrizione**
Standardizzazione dei service contract	Va assicurata la standardizzazione dei service contract, curando il modo in cui le funzionalità sono espresse, la definizione dei datatype, del modello dei dati e delle policy. Vi deve essere un'attenzione costante alla ottimizzazione ed alla appropriata granularità dei servizi, al fine di assicurare servizi consistenti affidabili e governabili.
Loose Coupling	Va garantita l'indipendenza del disegno e l'evoluzione della logica di business di ogni servizio e simultaneamente l'interoperabilità con i consumer dei servizi
Astrazione	Il disegno deve assicurare che i servizi occultino il più possibile i dettagli interni della loro implementazione
Riusabilità	I servizi devono essere progettati e realizzati in modo da favorire la loro riusabilità, considerandoli come risorse dell'organizzazione il più possibile agnostiche rispetto ad un contesto funzionale specifico
Autonomia	I servizi devo minimizzare la loro dipendenza sia per quanto concerne la logica che per l'ambiente di implementazione
Flessibilità	I componenti dovranno essere in grado di adeguarsi ai mutamenti tecnologici ed all'interazione con altri progetti presenti e futuri

Denominazione	Descrizione
Capacità di integrazione	I componenti di servizio (service component) sono il punto di partenza di un progetto ampio e complesso e dunque dovranno essere in grado di integrarsi, dal punto di vista tecnologico, con informazioni prodotte in sistemi diversi. A tal fine i componenti dovranno essere in grado di interfacciarsi con altri sistemi utilizzando standard riconosciuti.
Modularità	I componenti dovranno essere progettati, sia per quanto riguarda la parte hardware che la parte software, in maniera modulare per garantire una loro naturale evoluzione ed integrazione con altri sistemi
Affidabilità, robustezza e disponibilità	Il sistema deve essere disponibile in modo continuativo (H24 e 7x7), rispondendo agli SLA concordati; il sistema deve poter continuare a funzionare con adeguati livelli di alta affidabilità sfruttando la sua modularità anche in condizioni non specificate nei requisiti e in presenza di errori locali senza propagare i guasti a tutto il sistema
Manutenibilità	I componenti dovranno essere facilmente manutenibili; a tal fine il disegno progettuale dovrà essere chiaro, la documentazione completa e dovranno essere utilizzati software di base e strumenti di sviluppo ampiamente diffusi o standard de facto
Accesso utente tramite Front-End web-based	Tutti i componenti dovranno utilizzare schemi standard di applicativi
Semplicità d'uso	Il Front-End dovrà minimizzare l'intervento umano massimizzando, in ogni caso, l'ergonomia dell'interfaccia utente e favorire la facilità di utilizzo, presentando un ambiente intuitivo corredato di help on-line anche contestuale. Nella sua progettazione andranno tenute presenti le interfacce utente degli applicativi attuali in modo da minimizzare, per quanto possibile, il disorientamento iniziale degli utenti

Tabella 3 - Obiettivi architetturali

3. Architettura Generale di Sinfonia

Per la gestione dell'intero ciclo informatico e decisionale di una realtà costituita da organizzazioni ad elevata complessità gestionale, operativa e di processo come le organizzazioni che, a livello regionale e provinciale, governano tutti i processi della Sanità Pubblica (territoriale ed ospedaliera), sono necessarie soluzioni operative, di controllo e decisionali che possano garantire una visione in tempo reale della situazione di andamento della spesa, del bilancio, degli eventi sanitari ed epidemiologici, monitorando, per ciascun fenomeno, ogni singolo aspetto, con livelli di dettaglio e di aggregazione flessibili e variabili sulla base delle esigenze dell'utenza.

Il Sistema Sinfonia oggetto di fornitura si colloca, in Regione Campania, in un contesto di informatizzazione regionale in cui l'insieme delle soluzioni applicative ed infrastrutturali per il governo dei processi sanitari risulta essere "*variegato*" (e complesso) per tecnologie e pluralità di sistemi adottati nell'ambito dei diversi domini ed organizzazioni sanitarie e con una elevata tendenza alla distribuzione dei sistemi sul territorio.

In questo contesto si colloca l'intervento di Sinfonia con i suoi obiettivi di ***accrescimento dell'interoperabilità*** e ***del livello di federazione*** tra sistemi (e tra componenti applicative) e di ***allineamento***, per l'intera organizzazione sanitaria, indipendentemente dai vincoli territoriali e di dominio organizzativo, ***degli obiettivi e dei processi***, già nelle fasi di progettazione dei servizi applicativi.

La risposta a tali obiettivi è rappresentata dalla implementazione di soluzioni architetturali orientate ai servizi (SOA), che consentono di realizzare nuovi applicativi ed integrare applicativi esistenti all'interno di un processo di ridisegno complessivo del sistema IT.

4. Architettura del Sistema Sinfonia (Gestione Flussi)

Per ogni istanza Sinfonia il software applicativo è distribuito sui seguenti tier:

- Presentation Tier
- Business Tier

4.1. Presentation Tier

Il Presentation Tier ha la responsabilità di presentare i servizi sia in forma programmatica (Web Services) sia come Web Application per i servizi applicativi e sia come report.

I componenti di questo tier sono:

- Presentation Logic Web
- Presentation Logic Web Services
- Report

4.1.1 Presentation Logic della User Interface

La Presentation Logic della User Interface implementa l'interfaccia Web dei sistemi ed ha la responsabilità della presentazione dei servizi applicativi tramite interfaccia Web (XHTML) ad un operatore accreditato tramite una Workstation dotata di browser web.

La sua implementazione si basa sul Web-tier di un Application Server JEE, costituito da un Web Server e un Web Servlet Container che costituisce il contenitore standard per i componenti di front end della tecnologia JEE: Servlet e Java Server Pages (JSP).

Questo componente si occupa del dispatching delle richieste HTTP provenienti dal browser web e provvede alla generazione dinamica delle pagine (X)HTML di risposta. Ha la responsabilità della uniformità dell'interfaccia grafica, della gestione del page flow e del mantenimento dello stato conversazionale con il client.

La generazione dinamica delle pagine (X)HTML di risposta ed il controllo del flusso delle pagine web generate dinamicamente avviene seguendo il modello definito dal pattern MVC (Model View Controller).

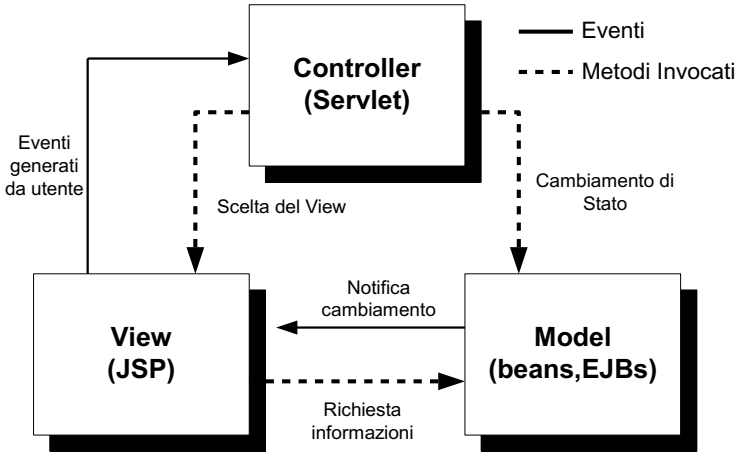

Figura 1 - Il Pattern MVC

In questo modello generale la Servlet (Controller) si comporta da motore web: in base all'input dell'utente, sul quale esegue una verifica di consistenza, decide quale processo di business invocare e seleziona la View successiva.

La View è realizzata attraverso pagine JSP che dinamicamente costruiscono il loro contenuto in base ai cambiamenti avvenuti nel Model, vale a dire recupera il risultato della transazione innescata dal Controller e lo visualizza all'utente.

Il Model è il sistema contenente la logica di business con cui l'utente interagisce innescando processi atti a conoscerne o alterarne lo stato.

L'uso del pattern MVC permette il completo disaccoppiamento fra la logica di presentation implementata nelle pagine JSP e la logica di controllo implementata nel codice della Servlet.

La specifica implementazione di MVC per i Servizi Applicativi prevede che:

- il Model renda disponibile il risultato di una transazione al Controller che a sua volta lo conserva nella sessione applicativa dell'utente;
- la JSP raccolga e renda visibile tale risultato all'utente titolare della sessione;

In particolare, il pattern è implementato mediante l'utilizzo del framework Spring MVC.

Nell'architettura dei servizi applicativi dei sistemi il ruolo del Model specificato nel pattern MVC è ricoperto, in linea con quanto dettato dal pattern Business Delegate, da un componente definito EJB Delegate a cui viene delegata la lookup, tramite JNDI, degli EJBs nell'EJB-tier che realizzano il Business Tier, disaccoppiando quindi in maniera completa la logica di controllo e di presentation dalla logica applicativa e di integrazione.

Rientra nella responsabilità del Controller la gestione del controllo di consistenza dei dati inseriti dall'utente e la gestione di situazioni anomale con presentazione all'utente di una pagina di errore. E' previsto l'uso di un Controller per ogni singolo caso d'uso individuato in fase di analisi delle componenti e, al fine di rendere più modulare e manutenibile il codice, le responsabilità del Controller sono distribuite su più classi di supporto.

I dati manipolati nello strato di *presentation* sono modellati da classi di business (Business Object) che rappresentano le entità del dominio.

Le pagine JSP fanno uso di codice JavaScript eseguito lato client, ad esempio per effettuare controlli sui dati inseriti dall'utente o per automatizzare interazioni tra l'utente e l'applicazione web. L'eventuale disattivazione del supporto JavaScript del browser non risulta comunque bloccante per l'applicazione.

Il controllo dell'accesso all'applicazione da parte dell'utente viene delegato a componenti applicative di Autenticazione e Autorizzazione Role Based secondo le modalità descritte nei relativi paragrafi.

Si riportano nel seguito le descrizioni dei pattern architetturali che saranno adottati per l'implementazione delle componenti della Web Application all'interno del Presentation-tier.

La tabella dell'Allegato 1, riporta i package della presentation logic con le relative responsabilità.

4.1.1.1 MVC e Business Delegate Web-tier

I pattern architetturali MVC e Business Delegate qui descritti vengono adottati per la realizzazione di tutti i casi d'uso che prevedono l'iterazione con l'utente mediante interfaccia web.

Tutti i casi d'uso sono realizzati coerentemente con lo schema riportato in figura.

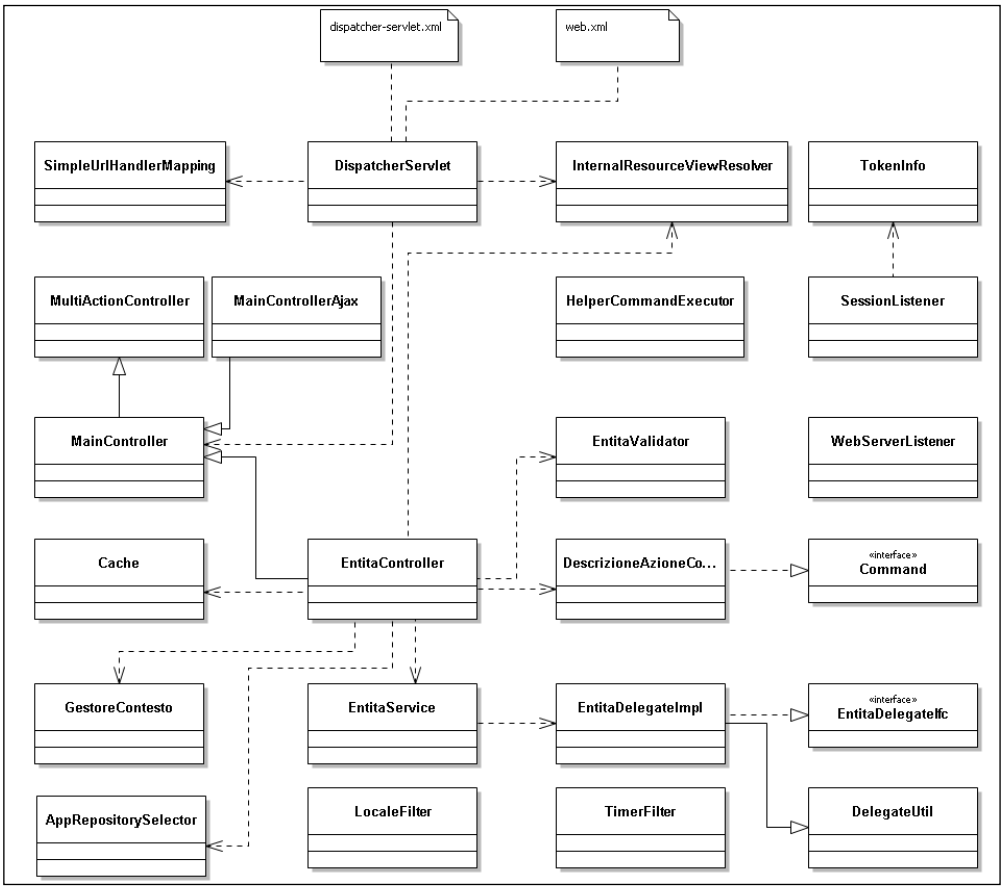

Figura 2 - Pattern MVC e Business Delegate

La tabella in Allegato 2 riporta la definizione delle responsabilità delle classi riportate in figura.

4.1.2 Presentation Logic dei Web Services

La Presentation Logic dei Web Services ha la responsabilità di esporre i servizi applicativi tramite interfaccia programmatica basata su standard SOAP, realizzati con tecnologia JaxWs.

Lo scheletro di un controller Spring JaxWs, con le relative annotazioni necessarie a renderlo un web service viene tipicamente costruito automaticamente dall'ambiente di sviluppo. Inoltre annotazioni aggiuntive consentono di espandere le funzioni infrastrutturali del servizio come ad esempio la gestione trasparente di aspetti come la gestione degli errori (fault), il log e la sicurezza.

Ciascun web service sarà quindi costituito delle seguenti componenti principali:

- Controller Spring JaxWs
- VO (Value Object)
- Ws Client (Se i sistemi invocano un web service JaxWs)

4.1.2.1 Controller Spring JaxWs

Per poter esporre un servizio di cooperazione mediante un web service JaxWs è necessario definire classi Java denominate Controller Spring JaxWs, che ne implementano il comportamento. Tali classi di implementazione fanno uso delle java-annotation standard Spring.

Ogni metodo del Controller JaxWs implementa una operation del web service, o meglio uno specifico servizio JaxWs. Il nome del metodo corrisponderà al nome del servizio JaxWs esposto e quindi un client che lo invocherà dovrà effettuare una chiamata utilizzandone quel nome di servizio.

4.1.3 Report

Per la realizzazione dei report viene utilizzato JasperReports, uno strumento open source sviluppato in Java in grado di produrre reportistica secondo numerosi formati: PDF, HTML, Microsoft Excel, RTF, ODT, CSV, XML, ecc..

Per la progettazione dei report sono disponibili diversi strumenti di disegno, sia stand-alone che integrati negli ambienti di sviluppo come Eclipse. Il modulo di runtime che si occupa della generazione dei report è integrato nello strato di presentation delle componenti applicative.

JasperReports consente di accedere ad una o più fonti di dati (data source), tipicamente database remoti, tramite la specifica di riferimenti, nella forma di stringhe di connessione standard, che utilizzano i driver presenti sul sistema in cui il software andrà in esecuzione.

4.2. Business e Data Tier

Il Business Tier ha la responsabilità di realizzare la logica di business dell'applicazione. L'organizzazione delle classi di questo strato è per entità.

Per ogni entità è stato definito un enterprise java bean (EJB) di tipo session stateless. In particolare, si utilizzano gli EJB3 che, a mezzo annotations, permettono di definire un EJB prescindendo da onerosi file di configurazione (ejb-jar.xml, jboss.xml), nonché di utilizzare un sistema di Object Relational Mapping (ORM) standard denominato Java Persistence API (JPA).

A ciascuna classe EJB sono associate opportune classi di supporto che, contengono la logica applicativa per i servizi di lettura e transazionali.

L'accesso al database da parte degli EJB avviene tramite specifiche indicate dalle JPA ed Hibernate è il provider individuato per la loro implementazione. Tutte le transazioni sono 'transaction-scoped' ossia, il contesto di persistenza viene propagato per tutta la transazione e ha vita fino a quando l'intera transazione non si conclude. Il contesto di persistenza viene creato quando il metodo del primo Stateless Session Bean viene invocato e la transazione finisce, con essa il contesto di persistenza, quando questo metodo termina.

Per l'implementazione della logica di business vengono utilizzati Session EJB di tipo Stateless per due ragioni:

- le richieste provenienti dal Presentation Tier sono di tipo stateless;
- gli Stateless Session EJB sono più efficienti e performanti.

In Allegato 3 si riportano i package che realizzano la logica di business di tutte le componenti applicative.

Si riportano nel seguito la descrizione del pattern architetturale adottato per l'implementazione delle componenti della logica di business delle componenti dei sistemi applicativi di cui trattasi.

4.2.1 Session Facade EJB-tier

Lo schema che segue rappresenta il pattern utilizzato per l'implementazione della logica di business.

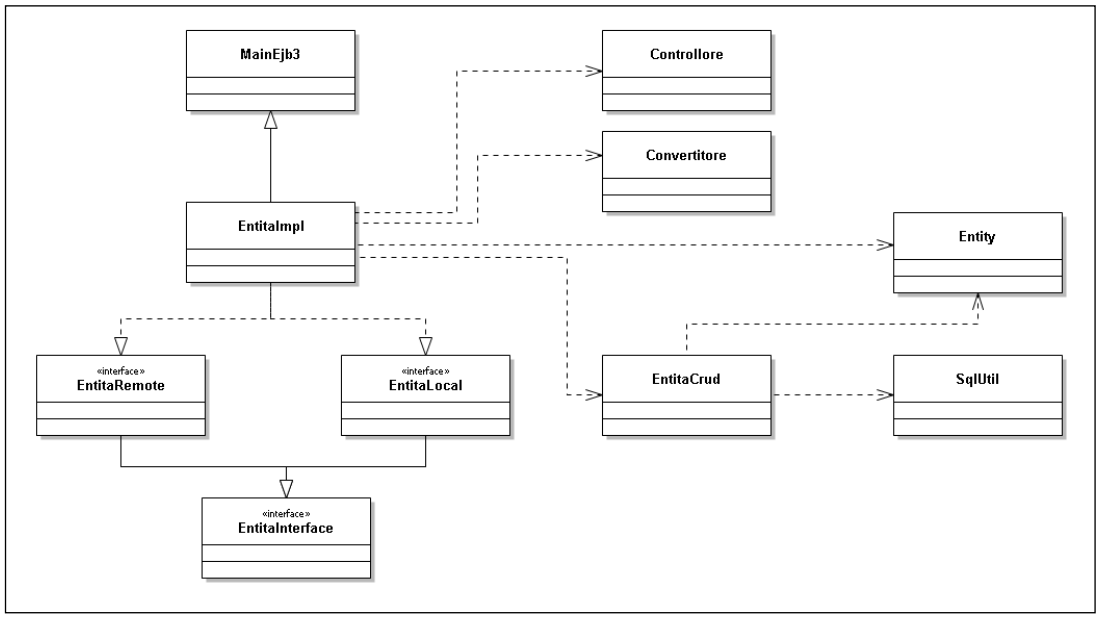

Figura 3 - Pattern Session Façade EJB-tier

La logica delle componenti che implementano l'EJB-tier è allocata nei package di cui all'allegato 4.

4.3. Elaborazioni Batch

Per elaborazione batch si intende un qualsiasi processo la cui esecuzione è asincrona rispetto alla richiesta attivata dall'utente mediante la web application e che durante la sua esecuzione non richieda interazione con l'utente. Pertanto non necessita di un ambiente operativo J2EE essendo sufficiente l'utilizzo di una JVM.

I casi d'uso che prevedono tali elaborazioni consentono all'utente, tramite interfaccia web, di richiedere una elaborazione batch consentendogli di esplicitare, se necessario, gli opportuni parametri di input. Successivamente un operatore di back office analizza le richieste pervenute e avvia l'esecuzione del processo batch. A processo concluso viene memorizzata su database l'avvenuta esecuzione del processo e l'esito (elaborato con successo o elaborato con errore). Lo stato della elaborazione viene reso disponibile all'utente mediante una funzionalità ad hoc.

L'autorizzazione dell'operatore di back office all'avvio di un processo batch è conseguente alla sua identificazione e autenticazione, mediante username e password, al sistema operativo ed al DBMS.

Spring Batch è un framework leggero che fornisce una solida base su cui costruire applicazioni batch robuste e scalabili.

Fornisce agli sviluppatori una serie di modelli collaudati che risolvono i problemi di batch comuni e consente agli sviluppatori di concentrarsi maggiormente sui requisiti di business e meno sulla complessità dell'infrastrutture batch.

Spring Batch contiene una grande varietà di componenti "out of box" configurabili che possono essere utilizzate per soddisfare la maggior parte dei più comuni casi di utilizzo batch. Una ampia configurazione XML e un modello di programmazione estensibile consentono una grande possibilità di personalizzazione delle componenti batch che possono quindi essere utilizzate come moduli per fornire rapidamente funzionalità comuni.

L'architettura del framework Spring Batch è quella degli ETL, ovvero Extract, Transform and Load.

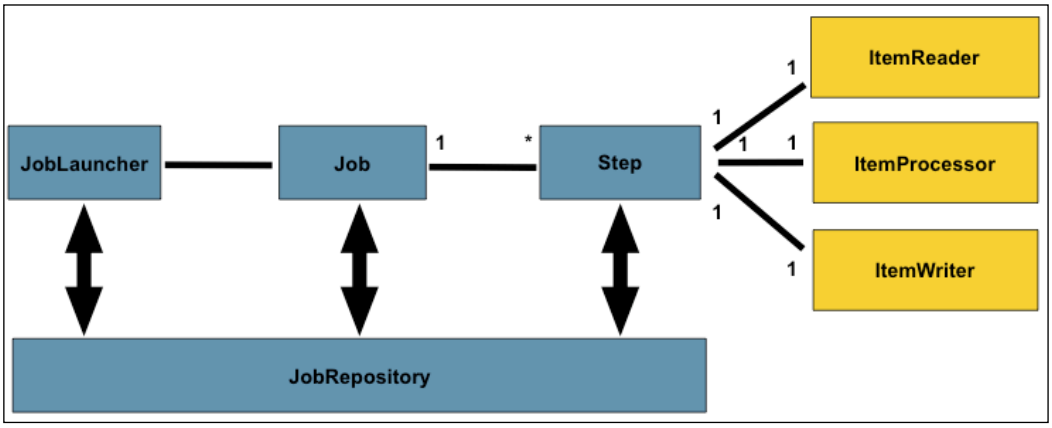

Figura 4 - Architettura Spring Batch

Ovvero un batch è definito come un Job (gestito da un repository), composto da n Step, ognuno dei quali esegue un processo di Lettura (Elaboration => ItemReader), Processazione (Transformation => ItemProcess) e Scrittura (Load => ItemWriter).

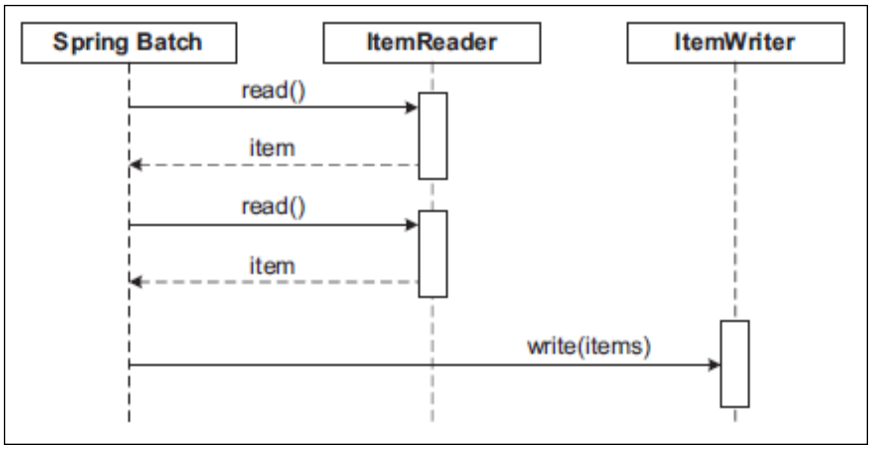

Figura 5 - Sequence Diagram Elaborazioni Batch

Dal punto di vista architetturale, le componenti che entrano in gioco nella richiesta e nell'esecuzione del batch sono distribuite su due layer:

- **Presentation Layer** che realizza i casi d'uso di richiesta di elaborazione batch;
- **Business Layer** che contiene la logica di start e di esecuzione del batch, che può essere un processo batch oppure un report batch, cioè un report non interattivo.

4.3.1 Presentation Layer

Il presentation layer è costituito dalle componenti di interfaccia web che consentono all'utente di richiedere l'esecuzione asincrona di un processo batch, fornendo gli opportuni parametri al processo. Tale richiesta, che è a tutti gli effetti un caso d'uso del sistema, viene memorizzata insieme ai parametri di input su database. In un momento successivo la richiesta viene presa in carico da un operatore di back office che avvia il processo batch, ne controlla l'esecuzione, ne analizza l'output e tramite interfaccia web può apporre un flag "visto" alle richieste evase nella tabella delle richieste dove è anche presente un flag di stato che prevede i seguenti valori:

1. "IN ELABORAZIONE" all'atto della richiesta di esecuzione del batch;
2. "ELABORATO CON SUCCESSO" dopo la corretta esecuzione del batch;
3. "ELABORATO CON ERRORE" se si sono verificati errori nella elaborazione del batch.

Ciascun processo batch provvede a registrare il proprio cambio di stato e produce un file di log consultabile dall'operatore di back office.

L'operatore che aveva effettuato la richiesta di esecuzione del processo batch può controllarne l'avvenuta esecuzione tramite interfaccia web, e, se previsto, eseguire il download del risultato del processo (report).

Dal punto di vista architetturale il presentation layer è del tutto simile ad un qualsiasi altro caso d'uso. Quindi per i casi d'uso di richiesta elaborazione batch valgono le scelte progettuali e architetturali effettuate per il presentation layer dell'intero sistema.

4.3.2 Business Layer

Il Business Layer delle elaborazioni batch si divide in due categorie diverse sia per il tipo di processo, sia per il risultato prodotto sia per la tecnologia adottata:

- **Processo Batch**: elaborazione che produce dati che vengono memorizzati sul db;

- **Report Batch:** elaborazione che produce file report in formato ASCII o pdf.

4.3.2.1 Processo Batch

Un processo batch:

- elabora dati presenti nel database in funzione dei parametri input forniti dall'utente che ha richiesto l'esecuzione del processo batch, anch'essi presenti nel database;
- produce risultati che vengono memorizzati nel database.

Un processo batch è costituito da un programma Java avviato da console, in un momento successivo alla richiesta, da un operatore di back office. E' un processo la cui esecuzione avviene all'interno di una macchina virtuale Java JVM standard J2SE. Per motivi di efficienza, dato il massiccio uso di accessi al database, la JVM di esecuzione può essere quella di una macchina in connessione intranet con Database Server se non una JVM presente sul database server.

4.3.2.2 Report Batch

Un report batch:

- elabora dati presenti nel database;
- l'elaborazione è in funzione dei parametri input forniti dall'utente che ha richiesto l'esecuzione del report batch, anch'essi presenti nel database;
- il layout e la logica di reporting del report sono definiti in un file con estensione .xml che risiede in un path accessibile dalla macchina in cui risiede la JVM di esecuzione del report batch;
- produce, come risultato della elaborazione un report, cioè un file di dati in formato conforme alle specifiche definite per il report; i dati sono disposti con un layout predefinito in fase di progettazione del report.

Il report batch è costituito da un programma Java avviato da console, in un momento successivo alla richiesta, da un operatore di backoffice, quindi è un processo la cui esecuzione avviene all'interno di una macchina virtuale Java JVM standard J2SE. Per motivi di efficienza, dato il massiccio uso di accessi al database, la JVM di esecuzione può essere quella di una macchina in connessione intranet con Database Server se non una JVM presente sul database server.

Tale programma utilizza le librerie di BIRT per integrare nell'applicazione la generazione dei report.

Il file con estensione .xml, che definisce il layout di un particolare report, risiede in un path accessibile dalla macchina in cui risiede la JVM di esecuzione del report batch ed è il prodotto della fase di design del report.

Il design di ogni report viene eseguito con l'ausilio del tool di sviluppo Report Designer all'interno dell'interfaccia IDE (Interactive Development Environment) di Eclipse.

In allegato 5 vengono riportati i package che contengono le classi di reporting delle componenti applicative.

4.4. Gestione Utenti ed Integrazione con sistema di SSO

Il sistema consente di accedere a tutti i servizi offerti, con meccanismi di autenticazione basati su username / password o smart card crittografiche (CIE, CNS, CRS, etc.). Il sistema gestisce,

con un'interfaccia, la gestione applicativa di ruoli e profili, che sarà possibile scegliere in fase di accesso. Gli utenti delle singole applicazioni presenti in Sinfonia accedono al sistema tramite un unico Front-End Web, la cui implementazione e autenticazione viene demandata al WSO2 Identity Server che interagisce in maniera federata con il Single-Sign On (SSO) regionale. Si rimanda a tale paragrafo per ulteriori approfondimenti in merito.

4.4.1 Identificazione, autenticazione ed autorizzazione degli utenti

L'identificazione, l'autenticazione e l'autorizzazione costituiscono i passi del processo attraverso il quale una entità accerta la corretta, o presunta, identità digitale di un utente.

Tutte le componenti applicative di Sinfonia per la fase di identificazione e autenticazione si integrano con il sistema di SSO.

La componente *Gestione Utenti*, invece, fornisce i servizi di amministrazione necessari a definire e profilare utenti nonché i servizi per l'autorizzazione dell'utente all'utilizzo delle singole funzionalità/servizi e alla visibilità di dati sensibili. La componente inoltre ha la responsabilità di produrre la reportistica analitica e riepilogativa relativa all'utilizzo dei servizi, all'assegnazione dei ruoli ed alla distribuzione degli utenti rispetto a ruoli e aziende sanitarie.

4.4.1.1 Definizione e Profilazione degli Utenti

La definizione e la profilazione di un utente è basata sulla sua identità e sui ruoli, detti Ruoli Istituzionali, che l'utente può assumere all'interno di una o più strutture.

La funzionalità di definizione e profilazione dell'utente fornisce la possibilità, ad un operatore autorizzato tramite interfaccia web, di definire o modificare più corrispondenze fra identità dell'utente, Ruolo Istituzionale e struttura in cui quel ruolo viene ricoperto.

La definizione e profilazione dell'utente in questi termini pone le basi per il processo di autorizzazione basata su ruolo e rende il meccanismo utilizzabile sia nel contesto Regionale che nel contesto aziendale.

4.4.1.2 Controllo delle autorizzazioni utente nello strato web

Il processo di definizione delle autorizzazioni è fondato sui Ruoli Istituzionali ed alla attribuzione a ciascun Ruolo Istituzionale di uno o più Ruoli Operativi. Un Ruolo Operativo viene definito come raggruppamento logicamente coerente di servizi.

Il sistema autorizzerà l'utente alla fruizione di un servizio solo se tale servizio è associato al Ruolo Operativo attribuito al Ruolo Istituzionale ricoperto dall'utente stesso (assegnato nella fase di definizione e profilazione).

Nell'ambito dello strato di presentation è stato utilizzato il meccanismo di verifica delle autorizzazioni offerto dal framework Spring Security basato su specifiche annotazioni da impiegare nel codice sorgente dei Controller.

4.5. Sicurezza accesso ai dati su DB

Poiché il database contiene i dati, la sua protezione è un aspetto di centrale importanza. In generale è sempre opportuno adottare ulteriori meccanismi di sicurezza esterni al DB, ma comunque aggiuntivi a quelli tipici del RDBMS. Oracle protegge i dati lì dove vengono conservati, all'interno del database, garantendone la protezione a un livello estremamente

elevato. L'RDBMS Oracle offre numerose funzionalità di sicurezza, dall'autenticazione utente alla gestione del privilegio ed al controllo dell'accesso.

4.5.1 Identificazione, autenticazione ed autorizzazione

Gli utenti accederanno al database per il tramite dell'application server che si connetterà al database mediante un pool di connessioni ed utilizzando una specifica utenza. Pertanto il DBMS si *limiterà* ad identificare ed autenticare l'application server verificando le autorizzazioni (Grant) di accesso ai dati in base al ruolo operativo dell'utente.

Il database dei sistemi gestisce il sistema delle autorizzazioni verificando i privilegi assegnati dal database administrator ai ruoli operativi. Quindi, dopo la fase di identificazione ed autenticazione, l'utente può eseguire operazioni su un oggetto del database solo se è stato espressamente autorizzato dall'amministratore. Per garantire la sicurezza e la privacy dei dati, saranno accordati all'utente solo i privilegi di cui necessita per svolgere le proprie funzioni, secondo il principio del "privilegio minimo". Riassumendo, i sistemi sono provvisto di un doppio sistema di profilazione dell'utente: uno al livello applicativo (solo l'utente autorizzato ad una specifica funzione potrà utilizzare la relativa funzionalità dell'applicazione) e il secondo all'interno del database (pur autorizzato al livello applicativo, vengono accordati all'utente i particolari privilegi sui dati necessari allo svolgimento del suo ruolo). Quindi, qualora un utente del sistema riuscisse anche ad aggirare il sistema di autorizzazione dell'applicativo, non riuscirebbe ad utilizzare le funzionalità in quanto non avrebbe le necessarie autorizzazioni al livello di database. Tale sistema garantisce quindi una profilazione dell'utente robusta a garanzia del principio di necessità nel trattamento dei dati (art.3 codice della privacy) che costituisce la precondizione di qualsiasi Sistema Informativo per la garanzia dei dati personali.

4.6. Cifratura

Alcuni requisiti di legge richiedono particolari misure quando dati personali o identificativi siano abbinati a informazioni di tipo sensibile. Ad esempio, l'accesso al nome dell'assistito in quanto tale può non richiedere particolari precauzioni, ma la combinazione del nome o del dato identificativo con informazioni di tipo sensibile può richiedere ulteriori misure di sicurezza come la crittografia.

I meccanismi di cripting dei dati sensibili al livello fisico nel database difendono da eventuali attacchi alla sicurezza che dovessero sopraggiungere dall'esterno del database stesso (ad es. qualcuno che riuscisse ad accedere direttamente al livello di Sistema Operativo ai datafile del database bypassando tutti i meccanismi di sicurezza messi a disposizione da Oracle).

Per questa eventualità il sistema RDBMS si avvale della feature **"Oracle Transparent Data Encription**" mediante il quale si può implementare in maniera trasparente il processo di cifratura dei dati sensibili direttamente nel motore RDBMS. Tale meccanismo consente di applicare la cifratura in maniera selettiva su specifiche colonne oppure a livello di intero tablespace per proteggere tabelle, indici e altri dati con algoritmi di cifratura robusti (3DES o AES fino a 256 bits) e senza la complessità della gestione di chiavi di cifratura.

Inoltre, anche la cifratura all'interno della Base Dati, se pur un valido meccanismo di sicurezza, non risolve il problema del furto dei supporti contenenti i backup. Per risolvere questo problema, il sistema, mediante la option Oracle Advanced Security, consentirà la cifratura dei backup direttamente sul supporto di salvataggio rendendo indecifrabili le informazioni in essi contenute in caso di accessi fraudolenti ai supporti sui quali vengono salvati i backup.

Il sistema implementerà la cifratura dei canali di comunicazione tra il database server e gli application server mediante gli algoritmi di cifratura (SSL/TSL) messi a disposizione da Oracle.

Il sistema implementerà, inoltre, il mascheramento dinamico dei dati sensibili mediante l'utilizzo della feature "Oracle Data Redaction" inclusa nella option Oracle Advanced Security. Sarà possibile creare policy che specificano le condizioni che devono essere soddisfatte prima che i dati vengano mascherati e restituiti all'utente. Durante la definizione di tali policy, si potrà specificare quali colonne mascherare, il tipo di protezione che deve essere applicato (totale, parziale, random ecc.) ed i ruoli istituzionali ai quali il dato viene mascherato.

In alternativa, laddove l'utilizzo della feature "Oracle Data Redaction" non consenta di soddisfare pienamente il requisito funzionale del mascheramento dati, si procederà al mascheramento dinamico dei dati sensibili in maniera applicativa.

4.7. Disaccoppiamento tra dati sensibili e anagrafici

Oltre al tradizionale meccanismo di ruoli e privilegi ed ai meccanismi di cripting dei dati sensibili si è ritenuto opportuno adottare, nella quasi totalità dei casi, anche il meccanismo di disaccoppiamento logico dei dati.

Tale meccanismo è ottenuto disaccoppiando le tabelle contenenti dati sensibili da quelle contenenti dati identificativi e correlandole tra loro mediante l'utilizzo di "codici non parlanti" (con tale terminologia ci si riferisce a codici non esplicativi della semantica del dato o a codici possano ricondurre immediatamente alla semantica del dato) oppure, utilizzando sempre codici non parlanti nei casi in cui i dati identificativi dell'utente e le informazioni sensibili siano contenute nella stessa tabella (es. codice fiscale dell'assistito e i codici esenzione sono contenuti nella stessa tabella, ma questi ultimi sono codificati con una codifica del tutto interna al sistema e non conosciuta dall'operatore). Solo in rare eccezioni, a causa della grossa mole dei dati e dell'elevata attività transazionale correlata, si è deciso di non applicare il disaccoppiamento per non impattare pesantemente sulle performance del sistema e si utilizzano quindi soltanto i meccanismi di ruoli e privilegi e di cripting dei dati.

4.8. Tracciamento e Monitoraggio

La componente Tracciabilità e Monitoraggio fornisce servizi trasversali a tutte le componenti applicative, con l'obiettivo di raccogliere (per consentirne poi la successiva analisi) le informazioni riguardanti gli utenti che accedono al sistema, i servizi da essi richiesti, data ed ora della richiesta, modalità con cui accedono al sistema e fruiscono dei servizi, l'esito del servizio richiesto.

La componente ha la responsabilità di conservare traccia degli eventi di fruizione dei servizi offerti dalle componenti applicative. Le informazioni raccolte, opportunamente aggregate ed elaborate, permettono di:

- misurare i carichi di lavoro del sistema;
- monitorare il livello delle prestazioni (per ogni servizio il tempo medio di esecuzione);
- elencare le situazioni anomale;
- produrre rapporti sui servizi erogati relativamente ad aree applicative
- monitorare le modifiche ai dati del database.

Questa componente non ha responsabilità di monitoraggio sistemistico che viene delegato alle componenti di ambiente e di sistema.

4.8.1 Ambito del tracciamento

Sono oggetto di tracciamento i seguenti eventi:

- utilizzo del singolo caso d'uso, query, report;
- singola funzione elementare del caso d'uso laddove applicabile;
- utilizzo del singolo web service sia per web services di consultazione sia di tipo transazionale;
- operazioni di CUD sulle persistenze del sistema.

Relativamente agli use case di consultazione, alle query e ai report si provvederà a tracciare i dati riguardanti i filtri di ricerca/consultazione. Non verrà effettuato alcun tracciamento del risultato.

Per quanto riguarda il tracciamento delle operazioni CUD sulle persistenze, si provvederà a tracciare, per ogni tabella sottoposta ad attività di tracing quanto segue:

- nome della tabella soggetta a tracciamento;
- tipo di operazione (insert, update, delete);
- istanze della tabella prima della modifica oppure in caso di inserimento di un nuovo record l'intera istanza inserita; nel caso di cancellazione l'istanza cancellata;
- istanza successiva alla modifica, nel caso di modifica;
- id dell'utente che ha effettuato la modifica;
- data ed ora della modifica.

4.8.2 Punti di tracciamento

I punti di tracciamento per use case, query, report e web services sono allocati sul layer web.

Il seguente diagramma evidenzia, nelle componenti già descritte, i metodi dedicati alle funzionalità di tracciabilità e monitoraggio ottenute tramite l'utilizzo della libreria log4j.

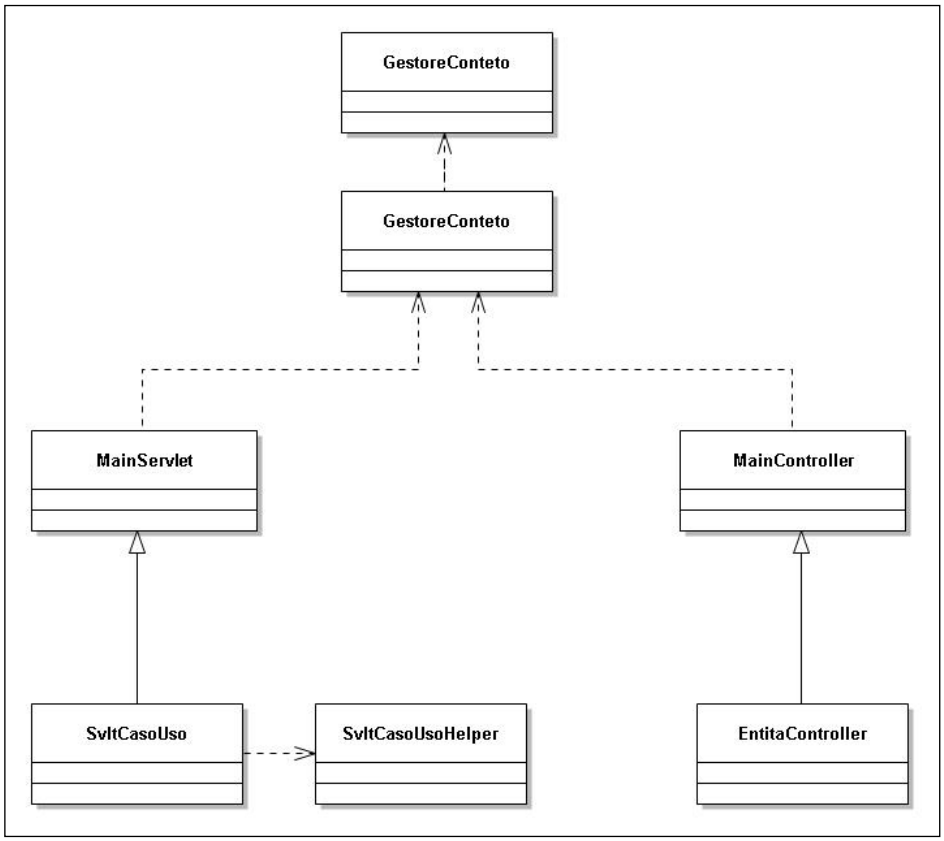

Figura 6 - Tracciabilità e Monitoraggio

In Allegato 6 vengono riportati i package che contengono le classi che hanno la responsabilità della gestione dei log applicativi.

4.8.3 Procedura di tracciamento

La strategia di tracciamento prevede due passi:

1. log su file (sul file system dell'application server);
2. procedura batch notturna che legge i file, inserisce i record di tracciamento in una apposita tabella del DB ed effettua il backup dei file.

4.8.4 Persistenza

Tutte le informazioni di tracciamento sono registrate in una apposita tabella del DB. Questa tabella è il punto di raccolta di tutte le informazioni dei canali di tracciamento. Le informazioni di auditing sono memorizzate su un'altra tabella del DB.

4.8.5 Canali di tracciamento

Per canale di tracciamento si intende il flusso di informazioni riguardanti una componente del sistema.

È definito un canale di tracciamento per ogni componente applicativa. Ad un canale di tracciamento corrisponderà uno specifico file che conterrà tutte le informazioni tracciate dal

sistema secondo quanto definito dalle regole **Ambito del Tracciamento** e **Record di Tracciamento.** Dunque ogni componente software che contiene punti di tracciamento utilizzerà il canale di tracciamento della componente applicativa di appartenenza.

4.8.6 Record di tracciamento

Il singolo record di tracciamento contiene, per ogni evento, i seguenti dati:

1. il momento esatto in cui si è verificato l'evento (data, ora, minuti e secondi);
2. l'identificativo dell'operatore che lo ha generato;
3. l'identificativo della sessione http gestito dal web server (jboss) in corso;
4. l'identificativo della transazione in corso, determinato dal software applicativo;
5. il nome del caso d'uso, query, report o web service;
6. il nome della pagina attraversata;
7. il nome dell'operazione (RICERCA, INSERIMENTO, CANCELLAZIONE, MODIFICA, DETTAGLIO);
8. il flag inizio esecuzione operazione;
9. il flag fine esecuzione operazione;
10. il flag esito operazione;
11. i valori della richiesta, nel caso di consultazione;
12. l'eventuale stack-trace dell'eccezione.

4.9. Funzionalità e meccanismi per la configurazione applicativa

Nella conduzione di sistemi informativi può essere necessario intervenire attraverso una *console amministrativa* per modificarne il comportamento senza necessariamente modificare il software applicativo che realizza funzioni e servizi.

La componente *Amministrazione Applicativa* fornisce gli strumenti per configurare e personalizzare il sistema, in tutti quei casi in cui l'implementazione permetta di scegliere il comportamento desiderato tra più opzioni disponibili. Le funzioni incluse in questa componente, dipendentemente dal loro ambito di applicazione (componente applicativa, intero sistema), sono disponibili tramite interfaccia web, rispettivamente ad un soggetto avente il ruolo di amministratore di sistema o di componente applicativa.

L'amministrazione del sistema, nei termini appena descritti, consente la gestione di opportuni parametri mediante i quali discriminare tra diverse opzioni disponibili per modificare i comportamenti, oltre che dell'intero sistema (nei casi in cui è applicabile), dei servizi e delle funzionalità di ciascuna componente applicativa.

Tutte le operazioni necessarie alla gestione sono eseguite senza interruzioni dell'erogazione del servizio: i parametri di configurazione sono pertanto modificabili a run-time.

Per consentire lo svolgimento di specifiche attività – quali ad esempio l'aggiornamento della base dati - l'area Amministrazione Applicativa consente di sospendere in maniera selettiva l'erogazione dei servizi di una specifica area applicativa, senza interrompere i servizi delle altre aree.

L'area implementa componenti e metodi richiamabili dalle diverse altre aree applicative per la lettura dei valori dei parametri di configurazione. La lettura dei valori dei parametri può avvenire a diversi livelli del software:

- nello strato WEB le componenti di tipo *it.exprivia.secsisr.<sistema>.<sigla area>.web.componente.servlet.casouso.SvltCasoUsoHelper* (helper dei casi d'uso delle altre aree applicative) accedono alla classe it.exprivia.secsisr.<sistema>.<sigla area>.web.proxy.parametroconfigurazione.DelegatoParametroConfigurazione.java
- nello strato EJB le componenti di tipo *it.exprivia.secsisr.<sistema>.<sigla area>.ejb.entita.bean.EntitaEJB* (EJB locali di entità) accedono alla classe it.exprivia.secsisr.<sistema>.<sigla area>.ejb.entita.dao.ParametroConfigurazioneDao
- nei batch che girano nella JVM di Oracle le componenti di tipo *it.exprivia.secsisr.<sistema>.<sigla area>.batch.areaapplicativa.batchcasouso.BatchCasoUso* (classi main delle elaborazioni batch) accedono alla classe it.exprivia.secsisr.<sistema>.<sigla area>.ejb.entita.dao.ParametroConfigurazioneDao

Il seguente diagramma mostra le relazioni fra le diverse componenti, nel rispetto delle naming convention e dei pattern adottati e già descritti.

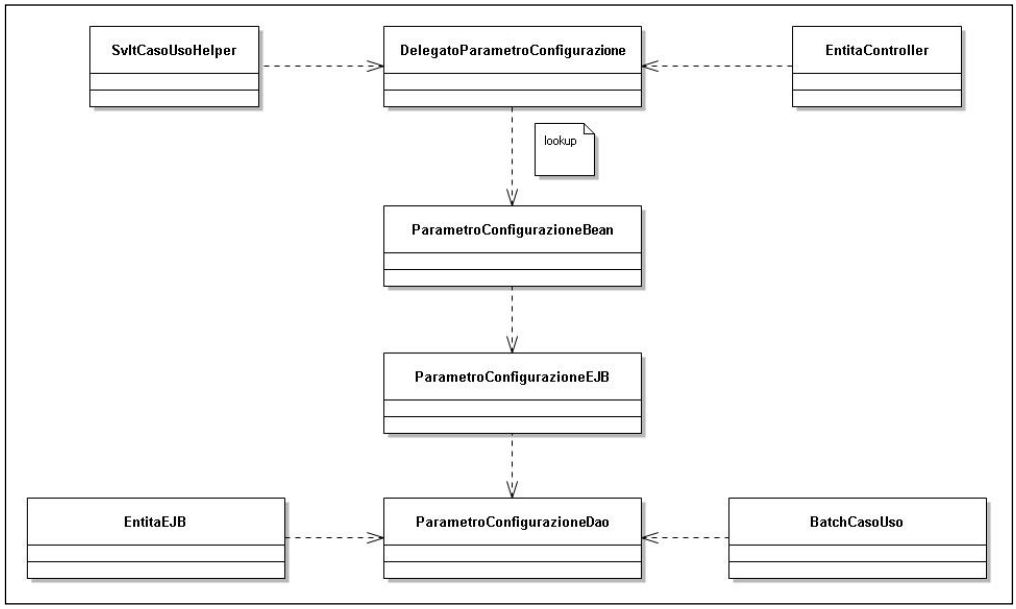

Figura 7 – Amministrazione Applicativa - relazioni fra le diverse componenti

4.10. Gestione delle Notifiche

Il trattamento di notifiche di documenti risponde all'esigenza di segnalare la creazione o modifica di una informazione, la modifica di un documento o la produzione di un nuovo documento da parte di un ente o amministrazione ad altri enti o amministrazioni.

La notifica documenti avviene con le seguenti modalità:

- registrazione e consultazione via web application con o senza allegati;
- via e-mail con o senza allegati;
- via e-mail con avviso di consultazione e download dell'allegato via web application.

Il presentation layer è costituito dalle componenti di interfaccia web che consentono all'utente di

- notificare un documento o evento;
- consultare le notifiche ricevute ed inviate e relativi download.

Dal punto di vista architetturale presentation layer e business layer sono del tutto simili a quelli di un qualsiasi altro caso d'uso. Quindi per i casi d'uso di notifica e consultazione eventi valgono le scelte progettuali e architetturali effettuate per presentation layer e business layer delle restanti componenti applicative.

Per quanto riguarda invece le notifiche a mezzo e-mail, tutte le componenti applicative si integrano grazie al modulo J-Communicator con il sistema di Posta Elettronica Certificata, consentendo agli utenti di poter fruire direttamente all'interno dei moduli applicativi web delle funzionalità di gestione della messaggistica mediante caselle PEC.

Per maggiori informazioni sul modulo JCommunicator si faccia riferimento al par. 8.3 **PEC**, posta elettronica certificata.

5. Anonimizzazione e Pseudonimizzazione di flussi informativi

La componente di Anonimizzazione e Pseudonimizzazione è una componente al servizio di tutto il sistema Sinfonia, che provvede a gestire i processi tecnici ed amministrativi connessi con le problematiche di anonimizzazione e di pseudonimizzazione dei dati sensibili e giudiziari.

Si tratta di un sistema di supporto a tutto il sistema Sinfonia in tutti quei i casi in cui risulterà necessaria, in accordo con il modello organizzativo e di processo e delle specifiche funzionali, la pseudonimizzazione di dati o gruppi di dati elementari, o la pseudonimizzazione di interi *frammenti verticali* di flussi informativi.

La componente consente di:

- generare un codice detto PILUR (Pseudonimo Identificativo Logico Univoco Regionale) e conservarne l'associazione con i dati identificativi diretti della persona, al fine di sostituire con tale codice i dati identificativi diretti del cittadino (pseudonimizzazione) all'interno flussi informativi contenenti dati sensibili;
- gestire le richieste di decodifica del PILUR;
- gestire le richieste di rilascio del PILUR a fronte di un codice fiscale;
- gestire le richieste cartacee di decodifica e di rilascio del PILUR;
- pseudonimizzare un flusso, ossia sostituire, in un flusso informativo, i dati identificativi personali del cittadino con il PILUR generato e la successiva registrazione in archivio dell'associazione tra PILUR e i dati identificativi personali.
- consentire la valutazione (accettazione/rifiuto) delle richieste di decodifica del PILUR e di rilascio del PILUR.

6. Dettagli architettura Gestione Flussi

6.1. Gestione Flussi

- La componente di Gestione Flussi è strutturata in layer architetturali concentrici, definiti da: **Layer di FrontEnd – per l'acquisizione delle informazioni tramite operazioni utente, la gestione e visualizzazione delle stesse, la richiesta dei flussi informativi;**
- **Layer di ESB/EMS – Enterprise Service Bus**, Enterprice Message Service per la configurazione di *gateway* di comunicazione in ricezione ed in trasmissione, nonché di *code* di lavoro JMS per i processi asincroni; **Layer di BPM – Business Process Management**, per la definizione di *work-flow* operativi più complessi;
- **Layer di ETL – Extract-Transform-Load**, funzionale alle attività di acquisizione, modifica e validazione dei dati in ricezione, di *data staging*, ed infine di predisposizione dei dati in trasmissione;

Alcuni moduli — laterali a tali *layer* — renderanno disponibili le funzionalità specifiche di:

- ***Protocollo*** — in termini di *logging* operativo — delle operazioni di ricezione e trasmissione.
- ***Archiviazione*** dei flussi informativi in ricezione ed in trasmissione.

La figura seguente rappresenta in termini schematici tali *layer* architetturali:

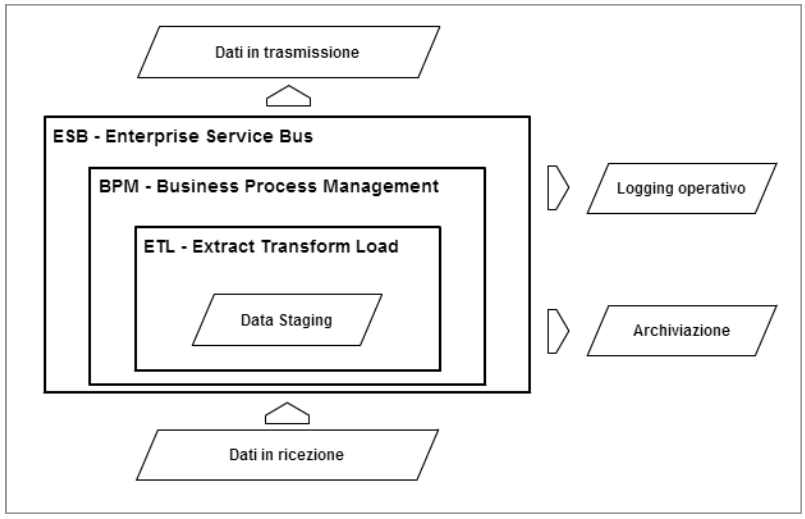

Figura 8 – Layer architetturali di Gestione Flussi

6.1.1 *Layer* di *FrontEnd*

Livello attraverso il quale si permetterà agli utenti di inserire a Sistema i flussi dati, di poterli modificare e gestire.

Sarà realizzato con AngularJS integrato in Liferay .

I benefici dell'adozione di questo strato sono:

- la facilità di visualizzazione e gestione per l'utente delle informazioni
- la possibilità di guidare l'utente nell'acquisizione e gestione dei dati inseriti
- la possibilità per l'utente di modificare le informazioni inserite a Sistema tramite un'interfaccia user friendly
- la possibilità per l'utente di recuperare tutti i file caricati direttamente tramite l'interfaccia Web, senza la necessità di dover accedere in altro modo a dischi di archiviazione.

6.1.2 *Layer* di *ESB – Enterprise Service Bus / EMS – Enterprice Message Service*

I processi di acquisizione dei dati più complessi dalle molteplici fonti informative - in presa diretta dal contesto operazionale regionale, attraverso cooperazione applicativa, o attraverso importazione di data file - saranno gestiti attraverso una architettura di enterprise service bus, che abiliterà al trasporto dei dati verso il layer di staging, semplificandone l'integrazione, tale layer verrà implementato mediante tecnologia TIBCO.

I benefici dell'adozione di una architettura di *enterprise service* bus sono:

- la separazione della *business logic* dai protocolli di comunicazione e dai formati di messaggio
- il *bridging* dei protocolli di comunicazione
- il *routing* dei messaggi basato su contenuti e regole di *delivering*
- la gestione del *payload* dei messaggi (*encryption*, *compression*, *encoding*, …).

Verranno create delle *queue* sull'EMS Tibco per permettere la comunicazione tra il FrontEnd e le diverse componenti, realizzando così il disaccoppiamento tra le stesse a fronte delle richieste effettuate dagli utenti al Sistema. Questo permetterà all'intera soluzione di essere più robusta a fronte di eventuali guasti.

6.1.3 *Layer* di *BPM – Business Process Management*

La definizione di processi di flusso — in termini di workflow dinamico piuttosto che di elaborazione statica — comporta l'implementazione di:

- *Policy* di schedulazione temporale dei dati in ricezione e di quelli in trasmissione
- registro dei mittenti e dei destinatari del processo trasmissivo
- conservazione in copia del flusso ricevuto e di quello corrispondente poi validato e trasmesso

- *Policy* specifiche e differenziate di gestione degli scarti di dato non valido: i flussi di dati che presentino scarti saranno notificati al mittente senza essere trasmessi al destinatario e potranno essere:
  - re-inviati (entro le date concordate) interamente dal mittente con le correzioni effettuate. Tale file subirà nuovamente il processo di validazione.
  - Modificati mediante form predefinite per la modifica parziale dei dati. Questi ultimi verranno risottomessi nel sistema per la validazione degli stessi e, in caso di esito positivo, trasmessi secondo le tempistiche e le modalità concordate.

6.1.4 *Layer* di *ETL – Extract-Transform-Load*

La ricezione, gestione, validazione e trasmissione dei flussi informativi saranno gestiti come processi *ETL* che prevedano:

- una fase di estrazione-ricezione dei dati da una o più sorgenti
- una fase di manipolazione dei dati — che comprende procedure di *data quality*, *assesment* e *cleansing*
- una fase di caricamento-trasmissione dei dati verso i destinatari finali.

6.1.5 Contesto infrastrutturale

La componente *Gestione Flussi* si colloca nel contesto infrastrutturale generale, secondo lo schema seguente:

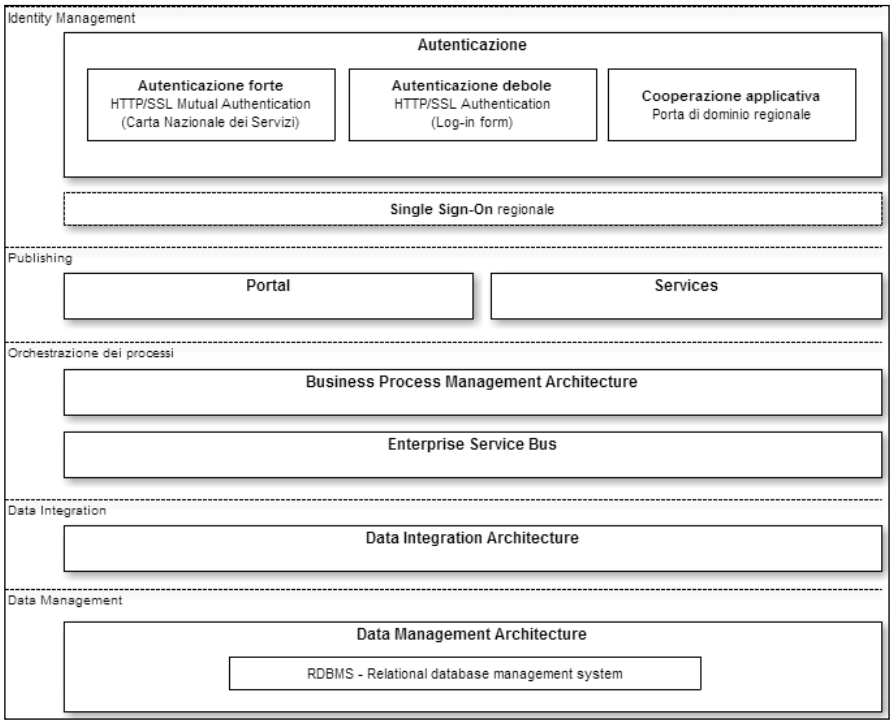

Figura 9 - Contesto infrastrutturale di Gestione Flussi

6.1.6 Entità funzionali di processo

Le entità funzionali di processo - in termini di flusso informativo - sono:

- **Flusso informativo in ricezione.**
- **Flusso informativo in trasmissione.**

Le entità funzionali di processo - in termini invece di processo - sono:

- **Processo di ricezione di flusso informativo.**
- **Processo di trasmissione del flusso informativo.**

6.1.6.1 Flusso informativo in ricezione.

Un flusso informativo in ricezione è definito da un set di *file* di *record* informativi riferiti ad uno specifico periodo di competenza, ed è caratterizzato da:

- un set di metadati quali ad esempio:
  - Denominazione del flusso informativo.
  - Periodo di competenza.
  - Azienda di competenza
  - Identificativo del mittente.

  - *Timestamp* di ricezione.

- File dei record di flusso informativo.

Per i sistemi esterni ogni file inviato, sarà considerato comunque come afferente a tutto il periodo di competenza. L'invio di un successivo file relativo allo stesso periodo e flusso informativo sarà considerato come sostitutivo del precedente.

6.1.6.2 Flusso informativo in trasmissione

Un flusso informativo in trasmissione è definito da un *file* di *record* informativi, caratterizzato da:

- un set di metadati quali ad esempio:
  - *Denominazione del flusso informativo.*
  - *Periodo di competenza.*
  - *Azienda di competenza*
  - *Identificativo del richiedente.*
  - *Timestamp di trasmissione.*
- File dei record di flusso informativo.

6.1.6.3 Processo di ricezione di flusso informativo

È il processo di ricezione — periodico — di un *file* di *record* informativi.

Il processo di ricezione è caratterizzato da un periodo di competenza e da un'azienda di competenza.

In questo periodo potranno esservi più eventi di ricezione del flusso: un evento di ricezione per il flusso iniziale, ed uno o più eventi successivi per flussi *sostitutivi*.

In tale intervallo temporale, inoltre, si potrà procedere con l'*editing* da operatore dei *record* di flusso informativo — in termini di operazioni di *update* e *delete* di *record* informativi specifici.

Dopo che l'utente preposto richiederà la generazione del flusso informativo, non potranno essere più ricevuti flussi sostitutivi né si potrà procedere con operazioni di *editing* da parte dell'operatore; qualora questo si renda necessario si dovrà procedere attraverso una procedura dedicata che è attivabile solo per tali finalità e da operatori preposti.

Il processo di ricezione dei flussi informativi è schematizzato nella figura seguente:

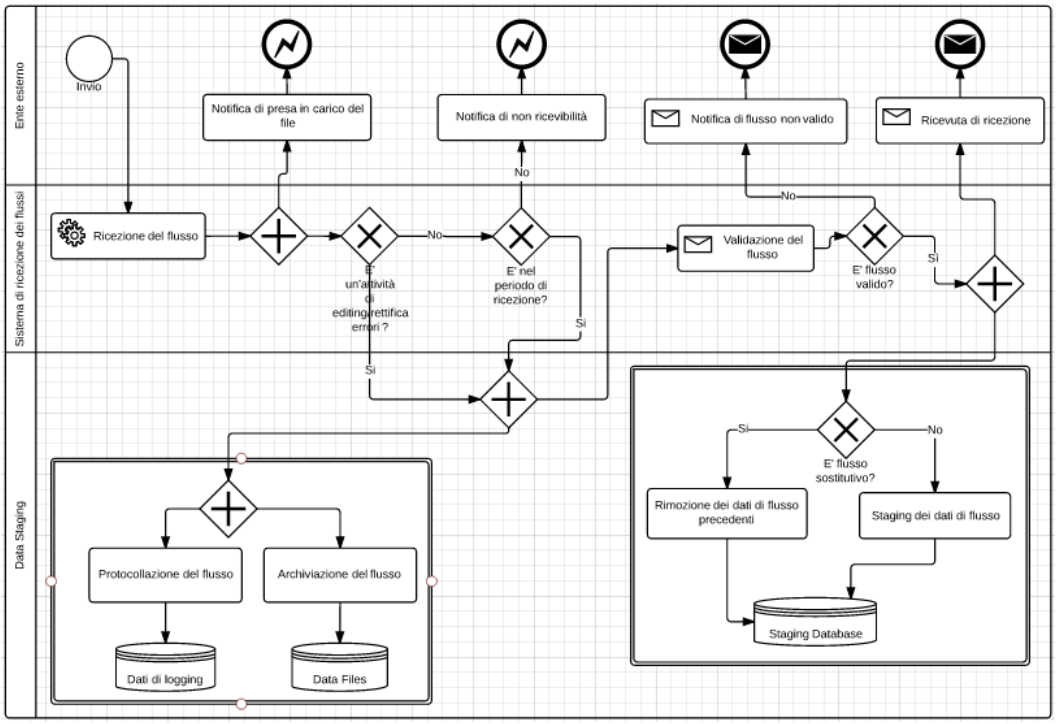

Figura 10 – Processo di ricezione di flusso informativo

Il processo di **ricezione** del flusso informativo si compone di tali eventi funzionali di processo:

- **Evento di ricezione - *file upload* - di flusso informativo**.
- **Evento di validazione di flusso informativo**.
- **Evento di editing da operatore di record del flusso informativo**.
- **Evento di validazione di record del flusso informativo.**

6.1.6.4 Evento di ricezione - *file upload* - di flusso informativo.

L'evento di ricezione è definito dall'*upload* di un *file* di *record* informativi:

- **Da operatore** - previa registrazione, attraverso un ***form* di *file upload*** reso disponibile dalla *web application* di gestione.
- **Da applicazione esterna** - attraverso la disponibilità di uno specifico ***web service* di tipo *SOAP Messages with Attachments*** (*www.w3.org/TR/SOAP-attachments*).

Nel contesto di un processo di ricezione si collocano uno o più eventi di ricezione in momenti temporali diversi compresi nell'intervallo in cui il processo di ricezione è aperto: un evento di ricezione per il flusso iniziale, ed uno o più eventi successivi per flussi *sostitutivi* dell'ultimo flusso ricevuto: **solo ove espressamente necessario si prevedono flussi — parziali — *integrativi***.

6.1.6.5 Evento di editing di alcuni record del flusso informativo

L'evento di editing è definito da operazioni di *update* e *delete* di *record* informativi specifici:

- **Da operatore** — previa registrazione, attraverso un ***form* di *editing r***eso disponibile dalla *web application* di gestione.

Nel contesto di un processo di ricezione si collocano uno o più eventi di editing in momenti temporali diversi compresi nell'intervallo in cui il processo di ricezione è aperto

6.1.6.6 Evento di validazione di flusso informativo

È l'evento di validazione di un flusso di dati in ricezione.

È differito - *asincrono* - rispetto all'evento di ricezione del flusso di dati.

Il *file* di *record* informativi verrà validato sintatticamente mediante XSD concordati che ne definiscono i vincoli:

- quali elementi ed attributi possono essere presenti, in quale relazione reciproca, quale tipo di dati può contenere (tipi di dati primitivi previsti dal formato XSD).
- definizione di nuovi tipi di dato partendo dai tipi primitivi attraverso tre possibili mecca*nis*mi:
  - *restrizione* (riduzione dell'insieme dei valori permessi);
  - *lista* (estensione ad una sequenza di valori);
  - *unione* (possibilità di scelta di un valore da differenti tipi).

L'evento di validazione di flusso informativo è schematizzato nella figura seguente:

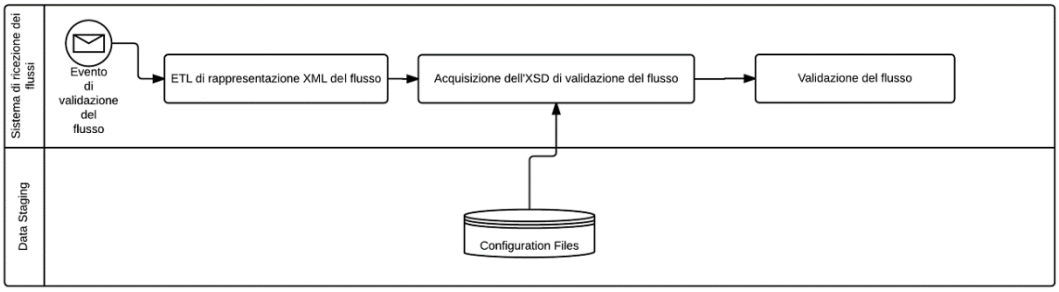

Figura 11 – Evento di validazione di flusso informativo

Il flusso informativo subirà, inoltre, un processo di validazione semantica secondo le regole esplicitate nel documento tecnico di specifica funzionale della componente flussi.

Tale regole, saranno applicabili se e solo le informazioni necessarie alla loro implementazione saranno messe a disposizione dagli enti preposti nella forma di:

- file (es: xml, txt, xls) acquisibili all'interno della soluzione
- mediante upload manuale

- condivisione di un'area predefinita.

Il processo di validazione effettuerà il controllo con gli ultimi dati disponibili all'interno della soluzione stessa.

Eventuali upload, successivi al processo di validazione, non saranno presi in considerazione salvo risottomissione manuale del processo di upload del flusso informativo (sostituzione del flusso informativo).

6.1.6.7 Evento di validazione di *record* del flusso informativo

La validazione di uno specifico *record* del flusso informativo è differita — a*sincrono* — rispetto all'evento di *editing* da operatore del *record*.

Alla fine del processo di validazione, il sistema provvederà a notificare all'utente lo stato della validazione effettuata sul record modificato.

6.1.6.8 Processo di trasmissione

È il processo di predisposizione del flusso informativo in trasmissione, e di *file downloading* di tale flusso.

Sarà possibile attivare il processo di trasmissione sono fronte di flussi di input privi di errori. Potrà comunque esservi un unico evento di trasmissione del flusso. Qualora si voglia ritrasmettere lo stesso, sarà necessaria un'operazione di "sblocco" flussi pubblicati da parte di un operatore autorizzato.

Il processo di trasmissione dei flussi informativi è schematizzato nella figura seguente:

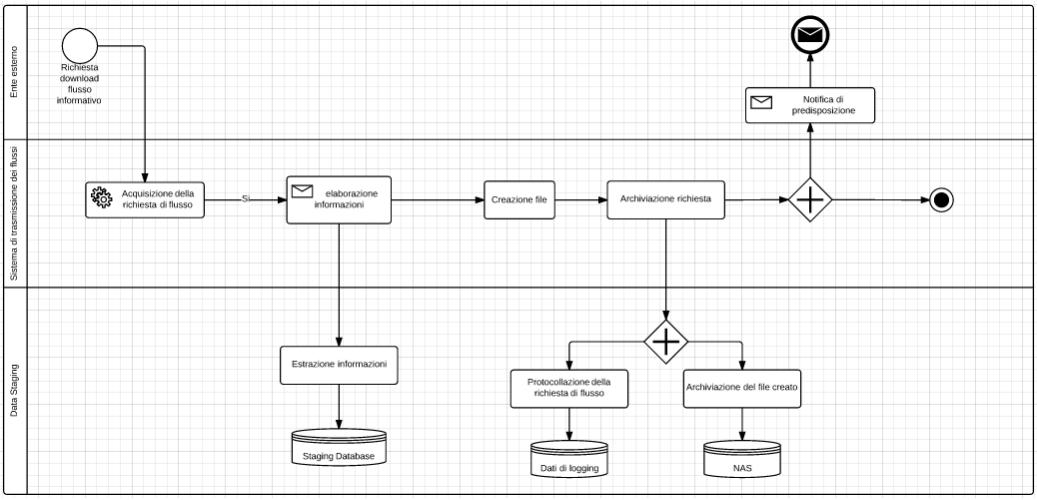

Figura 12 – Processo di trasmissione di flusso informativo

Il processo di **trasmissione** del flusso informativo è definito da tali eventi funzionali di processo:

- **Evento di predisposizione di flusso informativo**.

- **Evento di trasmissione - *file download* - di flusso informativo**.

6.1.6.9 Evento di predisposizione di flusso informativo

Attraverso specifica procedura *ETL* si produrrà il *file* di *record* informativi in trasmissione.

6.1.6.10 Evento di trasmissione - *file download* - di flusso informativo.

L'evento di trasmissione è definito dal *download* di un *file* di *record* informativi:

- **Da operatore** - attraverso un ***form*** **di** ***file download*** reso disponibile dal portale di gestione.
- **Da applicazione esterna** - attraverso la disponibilità di uno specifico ***web service*** **di tipo** ***SOAP Messages with Attachments*** (*www.w3.org/TR/SOAP-attachments*).

6.1.6.11 Ruoli di utenza

Gestione Flussi comporterà la definizione - nel contesto di *Identity Management* del portale dei servizi - dei **ruoli di utenza** di seguito indicati:

- Ruolo ***operatore in ricezione*** (*Azienda*) - autorizzato all'invio ed alla modifica di un flusso in ricezione.
- Ruolo ***operatore in trasmissione*** *(Dipartimento)* - autorizzato all'acquisizione di un flusso in trasmissione.
- Ruolo ***amministratore*** - Tale ruolo avrà la possibilità di monitorare tutte operazioni effettuate a Sistema ed ha entrambe le funzionalità dei ruoli "operatore in ricezione" ed "operatore in trasmissione".

7. Identificazione, autenticazione ed autorizzazione dei sistemi fruitori dei servizi

Obiettivo del capitolo è quello di illustrare i meccanismi e le specifiche con cui il sistema Sinfonia implementa i meccanismi di identificazione, autenticazione ed autorizzazione dei sistemi applicativi cooperanti che inoltrano richieste di servizio in modalità web services.

Nel seguito si intende per Sistema Fruitore un sistema applicativo che fruisce dei servizi di cooperazione di Sinfonia, esposti attraverso dall'ESB, che funge da Sistema Erogatore. Vengono considerati sistemi fruitori, alla stregua di qualunque altro sistema applicativo cooperante, le stesse componenti applicative ed i sistemi infrastrutturali di Sinfonia per le richieste di servizio che questi inoltrano verso le altre componenti applicative di Sinfonia.

L'identificazione, l'autenticazione e l'autorizzazione del Sistema Fruitore, per ciascun servizio di cooperazione esposto, sono implementati dall'ESB Tibco.

7.1. Il processo complessivo

Di seguito è illustrato il processo complessivo di interazione tra sistemi cooperanti relativi al processo di identificazione, autenticazione e autorizzazione nel caso di invocazione dei servizi esposti da Sinfonia da sistemi fruitori esterni al sistema Sinfonia.

1. Il Sistema Erogatore riceve un messaggio SOAP contenente il certificato X.509v3 del Sistema Fruitore in conformità alla specifica ”X.509 Certificate Token Profile” fornito da WS-Security. L’integrità del messaggio è garantita dalla firma digitale apposta con certificato X.509v3.
2. Il Sistema Erogatore verifica l’integrità sintattica del messaggio verificando la rispondenza all’xsd. In particolare viene estratto dal messaggio di input il token X.509v3, rappresentante il Sistema Fruitore. Successivamente si applicano tutti i controlli necessari a verificare la validità del certificato. Ottenuta la validazione del certificato, il Sistema Erogatore verifica che il common-name del certificato X.509v3 sia tra quelli autorizzati ad interagire con il Sistema Erogatore.
3. Il Sistema Erogatore, superati tutti i controlli del passo precedente ed in conformità con quanto definito nei successivi paragrafi relativi all’autorizzazione per i servizi di cooperazione, provvede ad erogare il servizio richiesto.
4. Il Sistema Erogatore accerta la conformità della richiesta applicativa rispetto alle eventuali politiche di sicurezza aggiuntive specifiche del servizio applicativo richiesto.
5. Il messaggio SOAP di response inviato al Sistema Fruitore soddisferà, analogamente al messaggio SOAP di request, la specifica “X.509 Certificate Token Profile” fornito WS-Security.

Nel caso l’interazione attraverso servizi web avvenga tra componenti applicative o infrastrutturali interne al sistema Sinfonia, al fine di ridurre l’overhead generato dall’applicazione delle policy di sicurezza previste dalla WS-Security, viene adottato un modello di sicurezza semplificato, bassato sull’utilizzo di SSL (Secure Socket Layer) in modalità “mutual authentication” sufficiente a garantire, oltre all’autenticazione dell’erogatore, anche l’autenticazione e l’autorizzazione del fruitore.

7.2. Identificazione ed autenticazione dei Sistemi Fruitori

L’identificazione e l’autenticazione del Sistema Fruitore esterno a Sinfonia è basata sull’utilizzo del certificato X.509v3 di autenticazione del Sistema Fruitore, secondo lo standard Web Services Security X.509 Certificate Token Profile (http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf).

L’identificazione del sistema fruitore deve individuare in modo univoco e certo lo specifico sistema che sta invocando il servizio esposto. Ciò significa che due installazioni distinte di uno stesso prodotto software, anche nello stesso dominio organizzativo ovvero anche sullo stesso sistema server fisico, sono identificate tramite due identità differenti e, quindi, tramite due distinti certificati di autenticazione X.509v3.

Ne consegue che ogni sistema fruitore deve essere dotato di un certificato X.509v3 il cui commonname deve essere censito nell’anagrafe dei certificati X.509v3 associati ai sistemi fruitori autorizzati ad interagire con il sistema erogatore.

Come da standard WS-Security, il certificato di autenticazione X.509v3 sarà utilizzato per la firma di parti del messaggio SOAP, in particolare dovranno essere firmate le seguenti porzioni di messaggio

- il tag <Timestamp>, previsto nell’header del messaggio SOAP;
- il tag <To>, previsto nell’header del messaggio SOAP;

- il tag <Action>, previsto nell'header del messaggio SOAP;
- il tag <MessageID>, previsto nell'header del messaggio SOAP;
- il tag <ReplyTo>, previsto nell'header del messaggio SOAP;
- il tag <Body>.

7.3. Integrità del messaggio

L'integrità del messaggio SOAP associato all'invocazione di un web service assicura che i messaggi non siano intercettati e alterati durante lo scambio fra Sistema Fruitore e Sistema Erogatore.

L'integrità delle parti fondamentali del messaggio è garantita sottoponendo a processo di firma:

- il tag <Timestamp>, previsto nell'header del messaggio SOAP;
- il tag <To>, previsto nell'header del messaggio SOAP;
- il tag <Action>, previsto nell'header del messaggio SOAP;
- il tag <MessageID>, previsto nell'header del messaggio SOAP;
- il tag <ReplyTo>, previsto nell'header del messaggio SOAP;
- il tag <AttributiAutorizzativi>, presente nell'header del messaggio SOAP;
- il tag <Body>.

7.4. Non ripudio del messaggio

Il non ripudio di un messaggio trasmesso dal Sistema Fruitore al Sistema Erogatore è garantito dall'autenticazione che una firma è in grado di offrire.

Infatti, l'univocità della firma digitale applicata ad un messaggio impedisce che il proprietario della firma disconosca le informazioni contenute nel messaggio firmato.

Il non ripudio del messaggio è garantito dall'applicazione della firma digitale da parte del Sistema Fruitore al messaggio SOAP-Request per:

- il tag <Timestamp>, previsto nell'header del messaggio SOAP;
- il tag <To>, previsto nell'header del messaggio SOAP;
- il tag <Action>, previsto nell'header del messaggio SOAP;
- il tag <MessageID>, previsto nell'header del messaggio SOAP;
- il tag <ReplyTo>, previsto nell'header del messaggio SOAP;
- il tag <AttributiAutorizzativi>, presente nell'header del messaggio SOAP;
- il tag <Body>.

7.5. Mantenimento delle informazioni della richiesta di servizio

Allo scopo di mantenere le informazioni relative alla richiesta del servizio, in maniera funzionale a dimostrare a terzi la legittimità dell'operato di Sinfonia, ove necessario, saranno memorizzati nel sistema i dati salienti dei messaggi scambiati tra Sinfonia ed i sistemi fruitori.

In considerazione delle ripercussioni che tale scelta può avere sul sistema in termini di occupazione dei volumi e di ulteriore carico transazionale, la definizione dei servizi per i quali saranno mantenute le suddette informazioni sarà effettuata congiuntamente con il committente.

7.6. Riservatezza del messaggio

La riservatezza del messaggio SOAP deve garantire che i dati trasmessi non siano alterati durante lo scambio e non siano interpretabili da alcuno con l'eccezione di chi ha il permesso di accedervi.

Lo strumento per garantire la riservatezza del messaggio è l'utilizzo di SSL (Secure Socket Layer), che permette di creare un canale protetto per lo scambio di dati tra due Sistemi.

Tutti i servizi di Sinfonia esposti come web services standard attraverso l'ESB sono fruibili su protocollo SOAP su HTTPS.

7.7. Firma dei messaggi di risposta

Per garantire integrità, non ripudio e riservatezza dei messaggi di risposta, nelle SOAP-Response saranno firmati, utilizzando il certificato X509v3 di Sinfonia, i tag:

- <Timestamp>
- il tag <To>, previsto nell'header del messaggio SOAP;
- il tag <Action>, previsto nell'header del messaggio SOAP;
- il tag <MessageID>, previsto nell'header del messaggio SOAP;
- il tag <RelatesTo>, previsto nell'header del messaggio SOAP;
- il tag <Body>.

7.8. Autorizzazione del Sistema Fruitore

Il Sistema Erogatore dopo aver autenticato e identificato il Sistema Fruitore verifica che quest'ultimo sia abilitato all'invocazione dei web services esposti dal Sistema Erogatore.

Il controllo si sostanzia nel verificare che il Sistema Fruitore abbia l'abilitazione ad interrogare i web services esposti dal Sistema Erogatore.

8. I Servizi Infrastrutturali

Al funzionamento del sistema Sinfonia contribuiranno i seguenti servizi infrastrutturali, che verranno dettagliati nel seguito del capitolo:

1. **Tibco**, Enterprise Message Bus
2. **Intalio**, Business Process Management System
3. **PEC**, posta elettronica certificata
4. **Firma Digitale**
5. **WSO2** Service Governance Registry

Prima di fornire una panoramica di ciascuno di questi strumenti software, è necessario chiarire il loro ruolo nell'architettura generale del sistema, cioè specificare come si relazionino a vicenda in modo da contribuire al funzionamento complessivo del sistema Sinfonia.

Dal punto di vista, dell'architettura orientata ai servizi (Service Oriented Architecture, SOA), gli strumenti software coinvolti sono essenzialmente il Business Process Management System (BPMS) Intalio, l'Enterprise Service Bus (ESB) Tibco e il Service Registry WSO2:

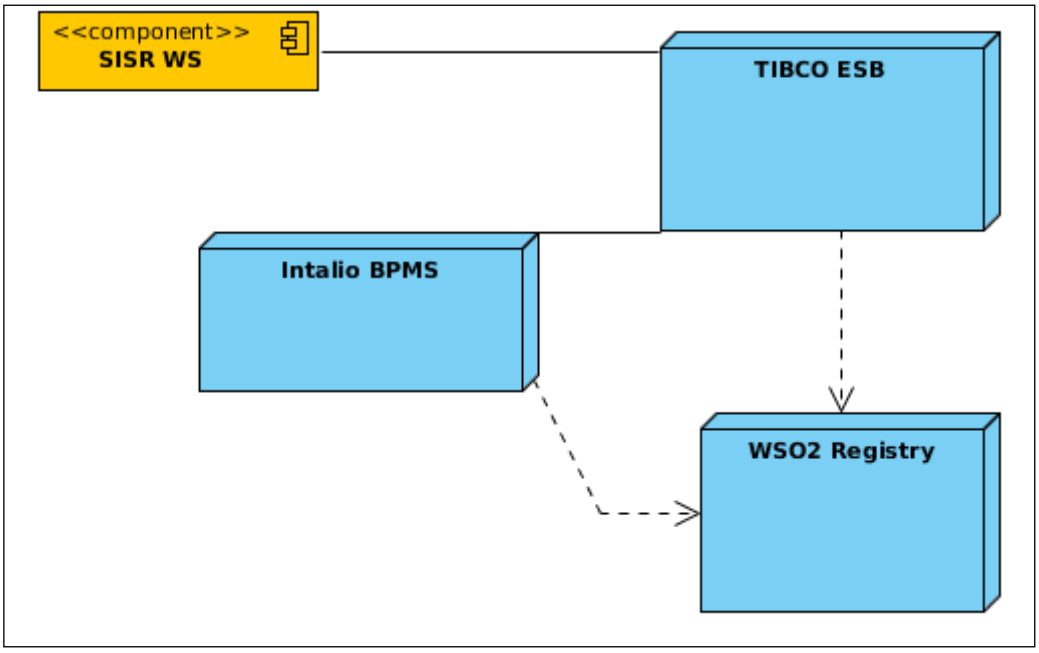

Figura 13 - Architettura SOA - Strumenti Software

I restanti due componenti infrastrutturali sono la Firma Digitale e la Posta Elettronica Certificata, che si integrano nativamente con i vari applicativi di Sinfonia.

8.1. Tibco

TIBCO Active Matrix è la piattaforma per costruire e dispiegare applicazioni SOA e comprende:

- il componente *Active Matrix Service Bus*, che include i Container SOAP, Mediation e Adapter e che servirà le Composite Applications (CA) che fungeranno da mediation routes tra sistemi diversi
- il componente *Tibco EMS* (Enterprise Message Service), basato su standard JMS
- il componente *Tibco Administrator*, che permette l'amministrazione dell'intera architettura SOA

L'interazione tra Tibco Active Matrix Service Bus e Tibco EMS permette la gestione di situazioni anche potenzialmente molto complesse, dove i connettori nativi tipicamente orientati ai servizi di Active Matrix (SOAP e REST) si possono integrare con il componente di messaggistica per garantire una QOS di livello elevato. Inoltre, la presenza dell'EMS permette di bufferizzare i messaggi per gestire carichi di lavoro anche importanti, oltre a garantire la possibilità di recapitare messaggi anche a subscriber momentaneamente non disponibili.

La soluzione proposta consentirà quindi di integrare i sistemi utilizzando qualunque Enterprise Integration Pattern (EIP), consentendo la realizzazione delle CA seguendo le best practices attuali.

Il template di processo ESB che consentirà l'integrazione tra due sistemi è quindi schematizzabile in questo modo

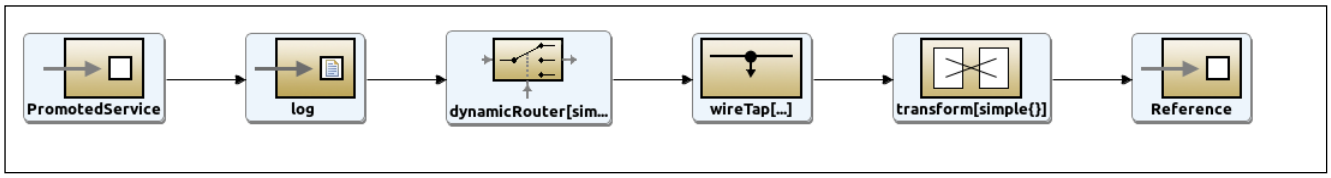

Figura 14 - TIBCO

Laddove:

- l'ESB promuove un riferimento al Web Service Destinazione, fungendo da proxy per quel servizio
  - il messaggio in ingresso viene loggato (Log)
  - del messaggio in ingresso viene calcolata l'eventuale destinazione sulla base dei dati al suo interno contenuti (Content-Based Routing)
  - viene effettuato un monitoring del canale (Wire Tap)
  - il messaggio in ingresso viene eventualmente trasformato (Message Transformation)
  - il messaggio viene recapitato alla destinazione, da cui si leggerà l'eventuale Acknowledge (sulla base dell'ACK restituito, il paradigma di scambio potrà essere In-Out o In-Only).

È importante notare che nello schema proposto è facilmente modificabile la QOS semplicemente inserendo un enpoint JMS (rappresentato, quindi da un messaggio consegnato su Tibco EMS) prima del promoted service, e/o prima della reference, in modo da garantire la consegna in ottemperanza della qualità del servizio concordata.

Nell'ambito dell'architettura proposta, Tibco si dovrà porre come punto centrale di scambio di messaggi, indipendentemente dal protocollo utilizzato: da questo punto di vista, il disegno seguente sintetizza la possibilità, offerta dal Service Bus, di tutte le comunicazioni all'interno del sistema, indipendentemente dal protocollo scelto per lo scambio di messaggi:

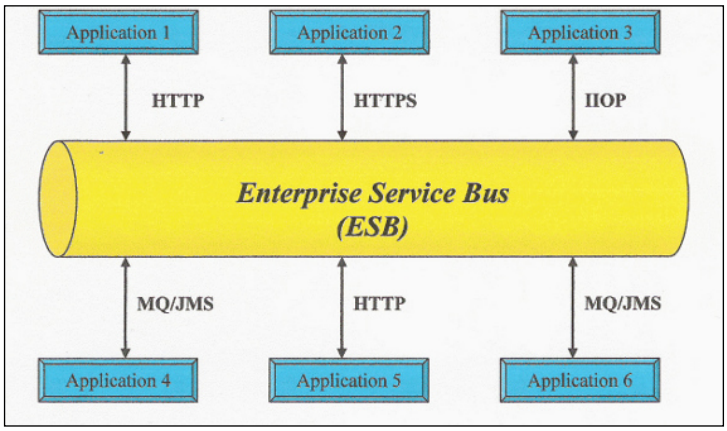

Figura 15 - Enterprise Service Bus

8.2. Intalio

La suite Intalio BPM è il un prodotto open source di Business Process Management, conforme allo standard BPM 2.0 e nativamente integrato con un motore di Business Rules (con la possibilità di impostare le regole direttamente nell'ambiente di designer). La piattaforma è costruita e basata attorno al modellatore standard BPMN STP di Eclipse e un motore Apache ODE BPEL, entrambi personalizzati da Intalio. Fornisce tutte le componenti necessarie per la progettazione, implementazione e gestione dei processi aziendali più complessi.

Intalio si interfaccerà sia con Tibco, ossia l'Enterprise Service Bus, sia direttamente con gli applicativi che potranno essere fonte di movimentazione dei processi di business. Tali applicativi, ovviamente, potranno anche essere notificati dell'avanzamento dei medesimi processi.

Intalio è utilizzato classicamente come orchestratore di processi SOA. Nel momento in cui un'integrazione di sistemi è realizzabile chiamando diversi servizi di diversi attori, e alla base di questa integrazione c'è una logica di business, tale integrazione è facilmente realizzabile attraverso un flusso di business rappresentato da uno schema BPM. Lo schema BPM permette essenzialmente di modellare decisioni di business semplicemente disegnando un diagramma, e consente ai sistemi coinvolti di contribuire al processo di business in accordo con l'orchestrazione modellata ed eseguita del server Intalio.

Lo schema seguente rappresenta graficamente il ruolo di Intalio nell'incapsulare la logica di business, oltre alla sua stretta integrazione con Tibco nel portare a termine l'orchestrazione dei servizi, sia interni che di partner esterni. Si noti come la logica di processo sia completamente all'interno di Intalio, mentre la parte di integrazione con altri servizi sia di esclusiva competenza di Tibco.

Altra cosa importante da notare di questo diagramma è che l'unica interfaccia di Intalio verso i servizi di cui è orchestratore è, in realtà, quella verso il sistema Tibco, che si incarica di fare da proxy per i servizi collaboranti e mantiene al suo interno le mediation routes verso i servizi stessi.

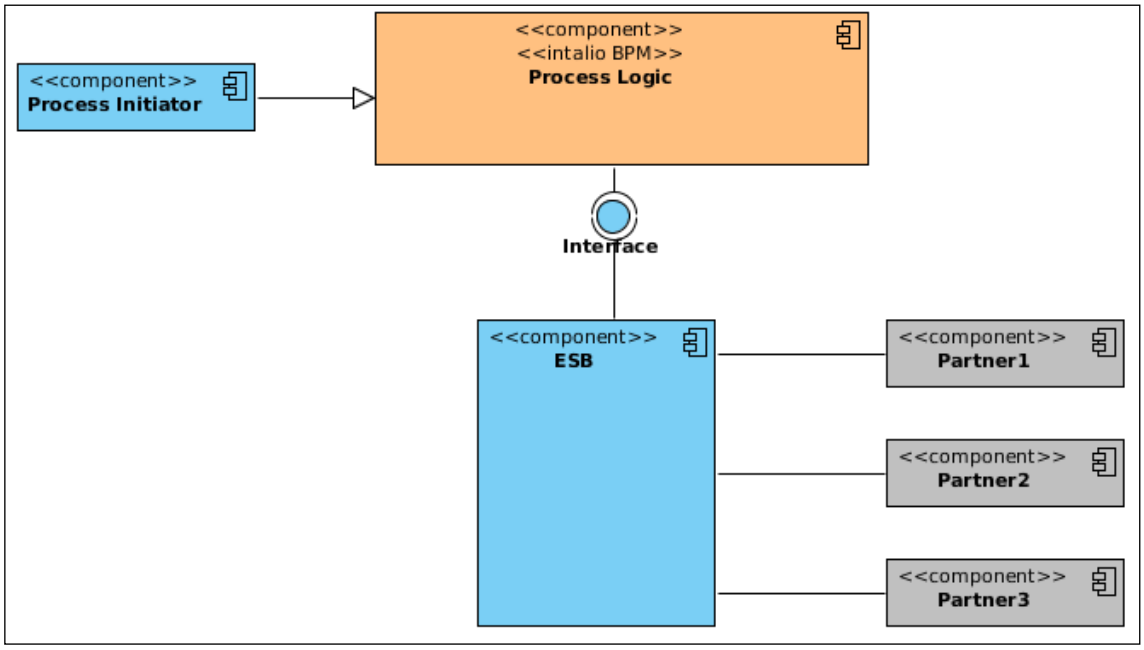

Figura 16 - Intalio

8.3. PEC

Il servizio infrastrutturale di PEC consente a tutti gli applicativi di Sinfonia l'invio e la ricezione di posta elettronica certificata.

La **Posta Elettronica Certificata** (PEC) è il sistema che consente di inviare e-mail con **valore legale equiparato ad una raccomandata con ricevuta di ritorno**, come stabilito dalla vigente normativa (DPR 11 Febbraio 2005 n.68).

Inoltre, il sistema di Posta Certificata, grazie ai **protocolli di sicurezza** utilizzati, è in grado di **garantire la certezza del contenuto** non rendendo possibili modifiche al messaggio, sia per quanto riguarda i contenuti che eventuali allegati.

La Posta Elettronica Certificata garantisce - in caso di contenzioso - l'opponibilità a terzi del messaggio.

Il termine "Certificata" si riferisce al fatto che il gestore del servizio rilascia al mittente una **ricevuta** che costituisce **prova legale** dell'avvenuta spedizione del messaggio ed eventuali allegati. Allo stesso modo, il gestore della casella PEC del destinatario invia al mittente la **ricevuta di avvenuta consegna.**

I gestori certificano quindi con le proprie "ricevute" che il messaggio:

- È stato spedito
- È stato consegnato
- Non è stato alterato

8.3.1 Il modulo di gestione PEC: J-Communicator

Il modulo J-Communicator è la componente trasversale che consente di gestire la messaggistica multicanale, quale l'invio/ricezione di mail, sms, fax; è predisposto per gestire anche l'invio e la ricezione di Posta Elettronica Certificata ed è in grado di elaborare migliaia di messaggi di PEC al giorno.

Il sistema è stato testato ed attivo con sistemi di PEC forniti ad es. da InfoCert, Actalis, PosteCert, ecc.

8.4. Firma Digitale

Il sistema di firma digitale fornito è integrato nativamente con il sistema di gestione documentale, consentendo di firmare e verificare qualsiasi documento. Nello specifico, le SmartCard utilizzate saranno emesse da Aruba e verranno consegnate assieme a un kit di firma digitale.

Il Kit per Firma Digitale sarà composto da:

- dispositivo sicuro di generazione delle Firme (Smart Card)
- lettore di Smart Card
- software di Firma e Verifica

Installato il Kit sul proprio computer, attraverso il Software di Firma sarà possibile selezionare il documento elettronico da sottoporre a Firma Digitale e, previa attivazione di un account, alla Marcatura Temporale.

Al momento della Firma del documento, il software chiederà l'inserimento del codice di protezione del dispositivo (PIN) che - se correttamente inserito - procederà con la creazione del file firmato digitalmente.

Il file firmato assumerà l'estensione .p7m che si sommerà all'estensione del file originario. Pertanto firmando un documento .txt, al termine del processo di Firma Digitale il documento assumerà l'estensione .txt.p7m che rappresenta una busta informatica (CADES o PADES).

Tale busta incorpora al suo interno il documento originario, il Certificato del sottoscrittore ed un Hash del documento firmato con il Certificato del sottoscrittore.

Tali componenti consentiranno, in fase di verifica della Firma da parte del destinatario del documento firmato, di accertare che:

- il documento non sia stato modificato dopo la Firma
- il Certificato del sottoscrittore sia garantito da una Autorità di Certificazione (CA) inclusa nell'Elenco Pubblico dei Certificatori
- il Certificato del sottoscrittore non sia scaduto
- il Certificato del sottoscrittore non sia stato sospeso o revocato

Se tutte le verifiche daranno esito positivo, il documento sottoscritto digitalmente potrà essere considerato valido a tutti gli effetti di legge.

8.4.1 Il modulo di firma digitale: J-Sign

Il modulo di firma J-Sign consente la firma e la verifica via web di qualsiasi documento digitale.

Il modulo è realizzato interamente in java ed è portabile su qualsiasi piattaforma (sistema operativo/browser), si interfaccia con qualsiasi smart card/token degli enti certificatori accreditati mediante le consolidate librerie PKCS#11.

Il modulo consente sia la firma nel formato P7M che nel formato nativo PDF, inoltre è già conforme alla recente normativa (Determinazione Commissariale 28 luglio 2010 che modifica la Deliberazione CNIPA n. 45/2009) di fatto è già compatibile con il formato CAdES e con l'algoritmo di hashing SHA-256.

Il modulo è integrato nel sistema documentale e verrà utilizzato in tutti i processi di gestione dei documenti digitali per cui l'Ente vorrà adottare la firma digitale.

Il modulo sarà adottato ad es. nel processo di Protocollazione, negli Atti (Determinazioni, Decreti, Delibere...), nella gestione della Fatturazione Elettronica e in tutti i processi documentali in cui l'Ente vorrà adottare la firma digitale.

Il modulo può essere utilizzato anche da sistemi esterni al documentale e integrato mediante l'invocazione di servizi web e la redirezione verso il servizio web di firma digitale.

8.5. WSO2

Con il termine Service Registry, in ambito SOA, ci si riferisce ad un sistema che contiene tutte le informazioni necessarie (come URL e modalità di accesso) al reperimento di tutti i servizi disponibili in esso registrati.

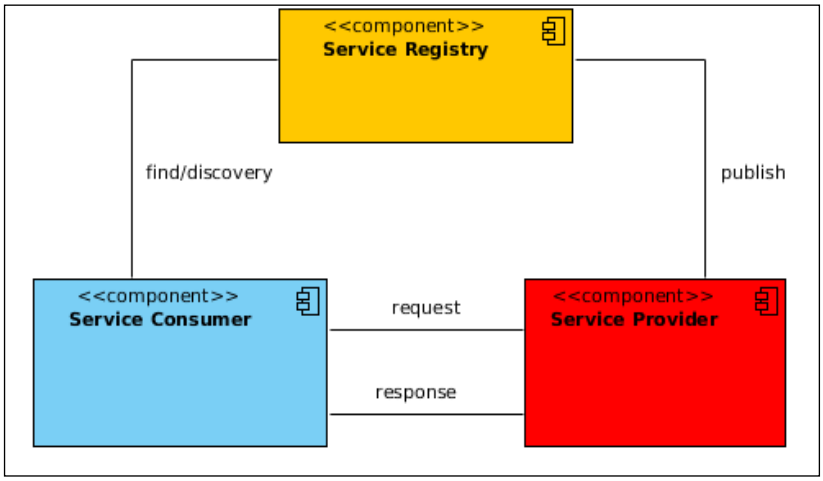

Figura 17 – Service Registry

Come si evince dallo schema sopra riportato, il vantaggio di un service registry è quello di disaccoppiare il service provider dal service consumer dal punto di vista della ricerca di un servizio e dal punto di vista della sua pubblicazione. Il prodotto scelto per espletare questa funzione all'interno dell'architettura SEC-SISR è WSO2 Governance Registry: si tratta di un prodotto 100% open source (licenza Apache 2) che consente di memorizzare, catalogare indicizzare e gestire i metadati dell'architettura SOA in un modo semplice e scalabile.

8.6. Deployment

Le componenti infrastrutturali Intalio BPM, Tibco EBS/EMS, OpenLDAP e Liferay descritte nei precedenti paragrafi sono ospitate ciascuna in un apposito nodo virtuale dell'infrastruttura di deployment di Sinfonia. Su ciascuno di questi nodi è presente la distribuzione Linux CentOS 6.6.

Allegato 1 - Package della presentation logic con le relative responsabilità

secsisr-<sistema>-<sigla area>-**web-condivisi.jar**	
Prefisso del Package	**Descrizione**
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi	Contiene le classi comuni al Web-tier per i diversi sistemi
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.cache	Contiene le classi che implementano la memorizzazione, nell'oggetto Session o in cache, dei dati utili all'interazione del caso d'uso.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.command	Contiene le classi che implementano la gestione del pattern command
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.contesto	Contiene e classi del web tier che implementano la gestione del contesto applicativo
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.controller	Contiene le classi del web tier che implementano funzionalità condivise da tutti i controller
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.filter	Contiene le classi del web tier che implementano la gestione dei filter applicativi
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.interfaces	Contiene i package dedicati alle interfacce del web tier
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.listener	Contiene le classi del web tier che implementano la gestione dei listener applicativi
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.report	Contiene le classi del web tier che implementano la gestione dei report birt
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.supporto	Contiene le classi del web tier che implementano la gestione di supporto applicativo (ad esempio logging)
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.ws	Contiene le classi del web tier che implementano la gestione di client per services jaxws
it.exprivia.secsisr.<sistema>.<sigla area>.web.util	Contiene le classi del web tier che implementano funzionalità aggiuntive di utilità

secsisr-<sistema>-<sigla area>-**delegate.jar**	
Prefisso del Package	**Descrizione**
it.exprivia.secsisr.<sistema>.<sigla area>.delegate	Contiene le classi delegate condivise da tutte le classi del Web-tier verso lo strato EJB-Tier
it.exprivia.secsisr.<sistema>.<sigla area>.delegate.common	Contiene le classi di supporto condivise da tutte le classi delegate che implementano il pattern business delegate verso lo strato ejb
it.exprivia.secsisr.<sistema>.<sigla area>.delegate.<entita>	Contiene le classi che implementano il pattern business delegate verso lo strato ejb per la specifica entità di business

Secsisr-<sistema>-<sigla area>**-web.jar**	
Prefisso del Package	**Descrizione**
it.exprivia.secsisr.<sistema>.<sigla area>.web.command	Dedicato alle classi che contengono la porzione di codice che effettua un'azione complessa
it.exprivia.secsisr.<sistema>.<sigla area>.web.controller	Dedicato ai Controller dei casi d'uso web
it.exprivia.secsisr.<sistema>.<sigla area>.web.service	Dedicato ai Service dei casi d'uso web
it.exprivia.secsisr.<sistema>.<sigla area>.web.validator	Dedicato ai servizi di validazione deputati ai controlli su dati delle pagine web dei casi d'uso web

Allegato 2 - Package per la realizzazione dei casi d'uso dei sistemi con le relative responsabilità

Nome	Descrizione
it.exprivia.secsisr.<sistema>.<sigla area>.web.validator.<Entita>Validator	Contiene i metodi che effettuano controlli sui dati di una specifica entità utilizzati delle pagine web e dal relativo controller dell'entità.
it.exprivia.secsisr.<sistema>.<sigla area>.web.controller.<Entita>Controller	Il Controller del pattern MVC, motore del page flow per la relativa entità di business dalla quale prende il nome.
it.exprivia.secsisr.<sistema>.<sigla area>.web.service.<Entita>Service	Classe service spring per il Controller dell'entità di riferimento che ne alleggerisce l'implementazione rendendo più strutturato, modulare e manutenibile il codice.
it.exprivia.secsisr.<sistema>.<sigla area>.web.command.<DescrizioneAzioneEntita>Command	Classe di supporto al Controller del caso d'uso corrispondente. Alleggerisce l'implementazione del Controller rendendo più modulare il codice. L'azione compiuta è strettamente legata al caso d'uso della specifica entità di business. it.exprivia.secsisr.<sistema>.<sigla area>.
it.exprivia.secsisr.<sistema>.<sigla area>.delegate.<entita>.<Entita>DelegateImpl	Il Model del pattern MVC ed elemento disaccoppiante fra la logica di business nello strato EJB ed il Controller secondo quanto dettato dal pattern Business Delegate. I metodi definiti sono it.exprivia.secsisr.<sistema>.<sigla area>.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.controller.web.MainController	Superclasse di tutti i controller web dei casi d'uso che raccoglie l'implementazione dei metodi a questi comuni.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.controller.web.MainControllerAjax	Superclasse di tutti i controller web dei casi d'uso con funzionalità asincrone Ajax che raccoglie l'implementazione dei metodi a questi comuni.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.controller.rest.RestCommon	Superclasse di tutti i controller rest dei casi d'uso che raccoglie l'implementazione dei metodi a questi comuni.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.controller.web.Ordina	Classe comparator di supporto per effettuare una comparazione di stringhe sulla base di una relazione d'ordine.
it.exprivia.secsisr.<sistema>.<sigla	Superclasse di tutti i validator dei casi d'uso che

area>.web.condivisi.controller.web.MainValidator	raccoglie l'implementazione dei metodi a questi comuni.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.cache.Cache	Classe per l'utilizzo dello strato di cache jboss infinispan utile per rendere l'applicazione scalabile e clusterizzabile a seconda delle esigenze di performance richieste e del carico elaborativo che il sistema deve sopportare. Nasconde tutti i dettagli implementativi della cache e consente di migliorare le performance.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.command.Command	Interfaccia da implementare per definire l'azione che lo specifico comando deve eseguire.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.command.HelperCommandExecutor	Classe di utilità che consente l'esecuzione immediata e sequenziale di comandi.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.command.OrdinaElencoCommand	Classe comparator di supporto per effettuare una comparazione di collection generiche tipizzate a runtime, sulla base di una relazione d'ordine.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.contento.GestoreContesto	Classe di utilità per la gestione e la memorizzazione dei dati del context applicativo.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.listener.SessionListener	Classe di gestione degli eventi associati al ciclo di vita della sessione web che esegue opportune operazioni al verificarsi di specifici eventi di sessione.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.listener.WebServerListener	Classe di gestione degli eventi associati al ciclo di vita del context applicativo che esegue opportune operazioni al verificarsi di specifici eventi del context.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.listener.TokenInfo	Classe utile per la memorizzazione e il tracciamento delle informazioni del client rest che effettua richieste json al server.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.supporto.AppRepositorySelector	Classe di utilità per la gestione del log applicativo implementato attraverso log4j.
Java Server Page Caso Uso	La View del pattern MVC. E' la pagina costruita dinamicamente sul server ed inviata al browser client. Vedi documentazione sulla tecnologia Java Server Page in J2EE.
org.springframework.web.servlet.DispatcherServlet	Servlet che si occupa di smistare tutte le richieste (POST, GET, ecc.) ai vari handlers, quindi funge fa Front Controller. La DispatcherServlet, essendo una servlet a tutti gli

	effetti, deve essere mappata nel file di configurazione “web.xml”. Vedi documentazione API spring-framework-3.2.3.
org.springframework.web.servlet.mvc.multiaction.MultiActionController	Rappresenta un controller generico di Spring che gestisce azioni multiple. Vedi documentazione API spring-framework-3.2.3.
org.springframework.web.servlet.view.InternalResourceViewResolver	Ogni Controller restituisce il nome logico di una view che viene risolto da questa classe.
org.springframework.web.servlet.handler.SimpleUrlHandlerMapping	Questa classe si occupa di mappare tutti gli URL ed il corrispondente Controller per gestire la richiesta di esecuzione di un flusso.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.listener.TokenInfo	Classe utile per la memorizzazione e il tracciamento delle informazioni del client rest che effettua richieste json al server.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.filter.TimerFilter	Classe filtro che consente al server di verificare quanto tempo il server impiega per smaltire una richiesta effettuata da un client.

Allegato 3 - Package che implementano l'EJB-tier con le relative responsabilità

Secsisr-<sistema>-<sigla area>-ejb-condivisi.jar	
Nome	**Descrizione**
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.condivisi.MainEJB3	Superclasse di tutti gli EJB che raccoglie i metodi che hanno implementazione comune.
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.condivisi.SqlUtil	Classe di utilità che consente di accedere a tutte le stringhe di query di CRUD esternalizzate dal codice della logica applicativa.
it.exprivia.secsisr.<sistema>.<sigla area>.vo.common.Pattern	Classe contenente i pattern utilizzati dalla logica di business

secsisr-<sistema>-<sigla area>-ejb.jar	
Nome	**Descrizione**
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.<entita>.<Entita>Crud	Classe di supporto all'EJB per le letture e le query transazionali di dati della specifica entità dal DB.
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.<entita>.<Entita>Interface	Superclasse delle interfacce Local e Remote. Contiene sia i servizi di business esposti all'esterno dell'EJB container tramite lookup via JNDI che quelli fruibili localmente nell'EJB container tramite lookup via JNDI
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.<entita>.<Entita>Remote	Interfaccia remota dell'EJB della specifica entità.
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.<entita>.<Entita>Local	Interfaccia locale dell'EJB della specifica entità.
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.<entita>.<Entita>Impl	Implementazione della logica di business del session bean stateless della specifica entità. Espone i servizi di business tramite lookup via JNDI.
it.exprivia.secsisr.<sistema>.<sigla area>.entity.<Entita>	Classe entity per una *entità* applicativa. Tali classi mappano le tavole del DB
it.exprivia.secsisr.<sistema>.<sigla	Classe value object condivisa che

area>.enums.<TipoEnumeratore>	rappresenta una entità di tipo enumerativo
it.exprivia.secsisr.<sistema>.<sigla area>.validators.Check<TipoValidatore>	Classe di Annotation che abilita la verifica di validità del tipo
it.exprivia.secsisr.<sistema>.<sigla area>.validators.Check<TipoValidatore>Validator	Classe di validazione preposta alla verifica di validità dello stato della specifica entità

Allegato 4 - Package che implementano le classi di reporting

Prefisso del Package	Descrizione
it.exprivia.secsisr.<sistema>.<sigla area>.batch	Contiene i package comuni ai processi batch
it.exprivia.secsisr.<sistema>.<sigla area>.batch.common	Contiene classi e package condivisi da tutti i processi batch.
it.exprivia.secsisr.<sistema>.<sigla area>.batch.jobs	Contiene le classi che rappresentano i jobs dei processi batch.
it.exprivia.secsisr.<sistema>.<sigla area>.batch.steps	Contiene le classi che rappresentano i gli step di Lettura, Processazione e Scrittura (ItemReader, ItemProcessor, ItemWriter)
it.exprivia.secsisr.<sistema>.<sigla area>.batch.tasklet	Contiene le classi che rappresentano i tasklet ovvero le scomposizioni di steps in unità più elementari per una più efficiente organizzazione.
it.exprivia.secsisr.<sistema>.<sigla area>.batch.chunks	Contiene le classi che rappresentano i chunk ovvero le scomposizioni di steps in unità più elementari per una più efficiente organizzazione.
it.exprivia.secsisr.<sistema>.<sigla area>.batch.bean	Contiene le classi di trasporto POJO.

Allegato 5 - Package che contengono le classi che hanno la responsabilità della gestione dei log applicativi

Nome	Descrizione
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.contesto.GestoreContesto	Gestisce i dati di contesto dell'applicazione web.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.servlet.MainServlet	Servlet astratta e quindi non istanziabile, superclasse di tutte le servlet dei casi d'uso e ne raccoglie l'implementazione dei metodi comuni.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.controller.MainController	Superclasse di tutti i controller dei casi d'uso e ne raccoglie l'implementazione dei metodi a questi comuni.
it.exprivia.secsisr.<sistema>.<sigla area>.web.area.casouso.CasoUsoController	Il Controller del pattern MVC, motore del page flow per il caso d'uso da cui prende il nome.
it.exprivia.secsisr.<sistema>.<sigla area>.web.condivisi.servlet.ServletHelper	Classe astratta e quindi non istanziabile, superclasse di tutte gli helper dei casi d'uso e ne raccoglie l'implementazione dei metodi comuni.
it.exprivia.secsisr.<sistema>.<sigla area>.web.componente.servlet.casouso.SvltCasoUso	Il Controller del pattern MVC. E' la servlet motore di page flow del caso d'uso da cui prende il nome.
it.exprivia.secsisr.<sistema>.<sigla area>.web.componente.servlet.casouso.SvltCasoUsoHelper	Classe di supporto alla servlet del caso d'uso corrispondente. Alleggerisce l'implementazione della servlet rendendo più modulare il codice.
log4J	log4J è una libreria Java sviluppata dalla Apache Software Foundation che permette di mettere a punto un sistema di logging per tenere sotto controllo il comportamento di una applicazione.

Allegato 6 - Package che contengono le classi che hanno la responsabilità della gestione dei parametri di configurazione delle aree applicative

Nome	Descrizione
it.exprivia.secsisr.<sistema>.<sigla area>.batch.areaapplicativa.batchcasouso.BatchCasoUso	Classe contenente il metodo “main” per l’avvio di un processo batch.
it.exprivia.secsisr.<sistema>.<sigla area>.web.proxy.parametroconfigurazione.DelegatoParametroConfigurazione.java	Il Model del pattern MVC ed elemento disaccoppiante fra la logica di business nello strato EJB e la servlet secondo quanto dettato dal pattern Business Delegate. Inoltre disaccoppia la logica di business dalla logica di accesso ai dati, implementata nel Data Access Object (DAO).
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.entita.dao.ParametroConfigurazioneDao	Data Access Object (DAO) per la relativa entità, incapsula l'implementazione delle query SQL definite nelle interfacce che implementa.
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.entita.bean.ParametroConfigurazioneBean	Session Ejb di facciata (facade): espone i servizi di business all'esterno tramite lookup via JNDI. Usa gli EJB local.
it.exprivia.secsisr.<sistema>.<sigla area>.ejb.entita.bean.ParametroConfigurazioneEJB	Session Ejb locale (local): espone i servizi di business agli Ejb di facciata tramite lookup locale al container.

REGIONE CAMPANIA – LINEE DI INDIRIZZO PER L'IMPLEMENTAZIONE DEL SISTEMA INFORMATIVO SANITARIO REGIONALE

ALLEGATO 2

FASCICOLO SANITARIO ELETTRONICO

"LINEE GUIDA DI INTEROPERABILITÀ

REGIONE CAMPANIA

SOMMARIO

INDICE FIGURE

ALLEGATO 2
FASCICOLO SANITARIO ELETTRONICO
“LINEE GUIDA DI INTEROPERABILITÀ

1. INTRODUZIONE

Il presente documento descrive le Linee Guida di Interoperabilità previste dall’Amministrazione Regionale al fine di sostenere la progressiva e sistematica digitalizzazione dei processi nel settore sanitario campano mediante l’implementazione di un modello unico che indichi l’uso delle tecnologie e gli interventi necessari. L’approccio adottato consentirà una centralizzazione non solo in termini tecnologici ma, soprattutto, di governance del processo di trasformazione digitale del sistema regionale nel suo complesso e, specificamente, del sistema sanitario regionale.

Il documento pone pertanto le basi per il raggiungimento dell’obiettivo di governance unitaria attraverso la creazione di un framework in grado di mettere a sistema il Fascicolo Sanitario Elettronico e SINFONIA ottenendo razionalizzazione, ottimizzazione e pianificazione delle infrastrutture telematiche, dei servizi ed ecosistemi digitali, delle piattaforme abilitanti e della relativa sicurezza informatica.

Il progetto denominato Sistema INFOrmativo Sanità Campania – SINFONIA prevede la costituzione di:

1. Anagrafe Unica Regionale Assistiti che si basa, come tutti i modelli di sanità elettronica, sul concetto di “paziente al centro”. L’Anagrafe Unica Regionale degli Assistiti rappresenta uno snodo centrale di tutte le informazioni di carattere anagrafico-sanitario dei cittadini su cui si appoggiano i servizi gestionali e di riconoscimento dell’assistito, rilascio TS, scelta e revoca del medico, di esenzione, ecc.
2. Anagrafe delle Strutture Sanitarie e Socio-Sanitarie che contiene l’anagrafica di tutte le strutture sanitarie, pubbliche e private accreditate della Regione. Essa consente di assolvere agli adempimenti della legge 326/2003 – articolo 50 e di catalogare in modo strutturato, tutte le strutture sanitarie regionali, i servizi disponibili, nonché tutte le informazioni utili per i cittadini e per gli operatori della sanità. L’archivio può essere agganciato anche ai sistemi regionali di georeferenziazione e svolge le seguenti funzioni:
   - viene referenziato dai servizi applicativi sanitari e socio-sanitarie e dalle applicazioni che gestiscono dati relativi alle strutture sanitarie regionali;
   - costituisce la fonte delle informazioni per la programmazione sanitaria regionale, grazie alle informazioni presenti sull’offerta dei servizi (posti letto, tipologie di prestazioni erogate, ecc.);
   - risponde a quanto previsto dal sistema nazionale di Monitoraggio della Rete di Assistenza (MRA);
   - fornisce i contenuti per la gestione dinamica di un portale sanitario regionale dedicato.
3. Anagrafe degli operatori sanitari che comprende tutti gli operatori sanitari che interagiscono nel sistema e che appartengono al sistema sanitario regionale, sia che essi lavorino in ambito pubblico, sia che essi lavorino in ambito privato. L’anagrafe deve fornire un insieme di servizi di identificazione del ruolo e dell’incarico che l’operatore svolge in una determinata azienda/struttura (anche ambulatoriale) e contestualmente al tempo a cui la richiesta di tale informazione si riferisce. Tali informazioni possono essere usate per profilare gli operatori sui diritti di accesso in lettura e scrittura ai sistemi in uso e per fornire un attributo di ruolo da associare ai

certificati per la firma digitale. L’anagrafe deve contenere informazioni relative alla persona fisica ed alla struttura di competenza ed altre informazioni utili che saranno meglio declinate nella fase di progetto operativo.

Le linee Guida definite per la presentazione dei Piani di progetto regionale per il (FSE), predisposte dall’Agenzia per l’Italia Digitale (AgID) ai sensi dell’art. 12 del D.L. 179/2012, hanno richiesto, quale componente abilitante per la realizzazione del FSE, la presenza di anagrafi degli assistiti, degli operatori e delle strutture di livello centrale regionale.

In ottemperanza a quanto richiesto dalle linee guida, la Giunta Regionale ha approvato la deliberazione n° 25 del 23/01/2018 con cui, tra l’altro, si prevede la razionalizzazione dei sistemi informativi sanitari regionali, attraverso l’unificazione e centralizzazione delle anagrafi di tutte le aziende sanitarie, al fine di rendere certificata ogni singola posizione anagrafica nel sistema regionale. Il sistema regionale dovrà inoltre allinearsi con il sistema nazionale di controllo della spesa farmaceutica e specialistica (Sistema TS) gestito dal Ministero delle Entrate e delle Finanze e con le nascenti Anagrafe Nazionale della Popolazione Residente (ANPR) e Anagrafe Nazionale degli Assistiti (ANA).

1.1. DEFINIZIONI E ACRONIMI

Termine	Descrizione
AgID	Agenzia per l’Italia Digitale
API	Application Programming Interface
BU	Business Unit
CdM	Comune di Milano
Consip	Consip S.p.a.
DoS	Denial of Service
EAP	Enterprise Application Pattern
ESB	Enterprise Service Bus
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technologies
IP	Internet Protocol address
IT	Information Technology
IoT	Internet of Things
IWA	Integrated Windows Authentication
JWT	JSON Web Token
OSGi	Open Service Gateway initiative
PA	Pubblica Amministrazione
PEP	Policy Enforcement Point
PSD2	Payment Services Directive 2
QoS	Quality of Service
REST	REpresentational State Transfer
RTI	Raggruppamento Temporaneo d’Impresa
SaaS	Software as a Service
SAML	Security Assertion Markup Language

SOA	Service Oriented Architecture
SPC	Servizio Pubblico di Connettività
SPID	Sistema Pubblico per la gestione dell'Identità Digitale
XACML	eXtensible Access Control Markup Language
WS	Web Services

Table 1 - Acronimi

2. CONTESTO DI RIFERIMENTO

Nell'ecosistema Sanità, ed in particolare nell'ambito del progetto Sinfonia, un ruolo centrale è ricoperto dal **Fascicolo sanitario elettronico (FSE)** che è lo strumento attraverso il quale il cittadino può tracciare, consultare e condividere la propria storia sanitaria. Il FSE unitamente alla costituzione delle anagrafi degli assistiti, delle strutture sanitarie e sociosanitarie e degli operatori, implementa il modello di interoperabilità 2018, di supporto alla strategia di interoperabilità e cooperazione tra le Pubbliche Amministrazioni, i cittadini e le imprese. La norma stabilisce che l'infrastruttura del FSE gestisca l'insieme dei dati e dei documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi riguardanti l'assistito.

La Regione Campania, oggi in regime di sussidiarietà, ha come obiettivo la piena applicazione del fascicolo sanitario elettronico entro il 2018. Un ruolo fondamentale nella diffusione del FSE sarà svolto dalle aziende sanitarie e ospedaliere.

"La Legge di Bilancio 2017 al fine di assicurare, un'omogenea diffusione nazionale del FSE ha variato il quadro di riferimento per gli scenari di evoluzione e diffusione del FSE con l'introduzione dell'Infrastruttura Nazionale per l'Interoperabilità (INI) dei Fascicoli Sanitari Elettronici regionali, nonché con la revisione di adempimenti e scadenze previsti per la realizzazione dei progetti di FSE da parte delle Regioni. Fermo restando quanto già previsto nell'ambito del D.P.C.M. n. 178 del 29/9/2015 "Regolamento in materia di fascicolo sanitario elettronico" e dalle specifiche AgID per l'interoperabilità tra i sistemi regionali di FSE, l'INI ha il compito di garantire l'interoperabilità dei FSE regionali e mette a disposizione una serie di funzionalità per l'alimentazione e la consultazione del FSE. L'infrastruttura nazionale, oltre a garantire i processi operativi per sistemi regionali di FSE esistenti, dovrà assicurare funzioni, nella loro interezza o in maniera modulare, per la realizzazione e gestione di un sistema di FSE per le regioni e province autonome che non hanno sviluppato completamente proprie soluzioni di FSE. (regime di sussidiarietà)[1]"
INI espone dei servizi che si possono suddividere nelle seguenti macro categorie:

- servizi di gestione e comunicazione dei consensi;
- servizi di gestione e comunicazione delle informative regionali;
- servizi di recupero dei metadati dei documenti che compongono il FSE;
- servizi di recupero dei documenti del FSE, compatibilmente con le politiche di accesso da parte di un assistito, un operatore o un professionista sanitario;
- servizi di comunicazione o di aggiornamento dei metadati relativi ad un documento o di cancellazione dei metadati di un documento invalidato;
- servizio di trasferimento dell'indice a seguito del cambio della regione di assistenza di un assistito.

In relazione allo stato di avanzamento dei propri FSE, le Regioni hanno aderito in toto o in parte al progetto INI. La Regione Campania, insieme alla Calabria e alla Sicilia, ha aderito in toto

[1] Conferenza Stato regioni, Contributo sullo stato di attuazione del FSE, 26 ottobre 2017.

all'infrastruttura nazionale di sussidiarietà. INI ha messo a disposizione di queste Regioni le principali componenti di storage dell'infrastruttura (repository e registry) e alcuni servizi tra cui:

- Autenticazione cittadini e professionisti sanitari;
- Gestione del consenso e oscuramenti documenti;
- Comunicazione dell'informativa;
- Consultazione FSE;
- Indicizzazione documenti;
- Archiviazione documenti;
- Consultazione accessi;
- Gestione e indicizzazione dei patient summary

Inoltre, ad integrazione dei contenuti minimi previsti dal DPCM 178/2015 (dati identificativi e amministrativi dell'assistito, referti, verbali pronto soccorso, lettere di dimissione, profilo sanitario sintetico, dossier farmaceutico, consenso o diniego alla donazione degli organi e tessuti), nell'ambito delle attività del Tavolo di monitoraggio FSE sono stati individuati come prioritari anche i seguenti contenuti:

- prescrizioni (specialistiche, farmaceutiche, ecc.);
- bilanci di salute;
- dossier farmaceutico;
- vaccinazioni;
- prestazioni di assistenza specialistica;
- certificati medici;
- esenzioni;
- prestazioni di assistenza protesica;
- promemoria ricetta.

I documenti e le informazioni cliniche di cui sopra dovranno prevedere i contenuti minimi ed essere resi disponibili in formato CDA2 secondo le specifiche che saranno prodotte dai gruppi di lavoro *ad hoc* recentemente costituiti nell'ambito dei tavoli tecnici nazionali (GDL).
Dal quadro di contesto sintetizzato in precedenza, discendono per le Regioni una serie di attività da porre in essere che sono sistematicamente monitorate dal livello nazionale.
Anche la Regione Campania, pur avendo aderito al regime di sussidiarietà, dovrà porre in essere un complesso coordinato di attività propedeutiche per adempiere alla normativa e popolare il FSE-INI. Tali attività dovranno essere volte a:

- creare le condizioni perché il FSE possa essere alimentato in modo completo, corretto e continuativo dalle strutture che producono i documenti, gestendo in modo coordinato il percorso di adeguamento tecnico ed organizzativo delle strutture stesse, pubbliche e private.
- organizzare in modo strutturato la fase di raccolta dei consensi presso i propri assistiti, individuando modalità e soluzioni organizzative efficaci;
- definire le strategie di coinvolgimento degli operatori in senso lato (MMG, PLS, farmacie….) nel percorso di attivazione del fascicolo;
- coordinare le attività di promozione e formazione rivolte a cittadini e operatori.

Tali attività risultano per altro necessarie non solo ai fini dell’alimentazione del fascicolo in regime di sussidiarietà, ma sono necessarie anche nel caso in cui la Regione decida di dotarsi di una propria infrastruttura di FSE adottando INI solo per l’interoperabilità.

3. ARCHITETTURA APPLICATIVA

3.1. HIGH LEVEL DESIGN

Da un punto di vista architetturale l’Infrastruttura di Interoperabilità messa a disposizione dall’Amministrazione si declina in tre componenti logiche a supporto della realizzazione dei servizi che ruotano intono al tema del Fascicolo Sanitario Elettronico:

1. **Api Governance:** L’esposizione dei servizi ai vari stakeholders interessati alla vita del FSE è mediata tramite uno strato di Api Management che consenta di gestire ed orchestrare le richieste per accedere alle API e i WS da parte di applicazioni e partner. Le funzionalità che dovrà rendere disponibile tale componente sono Progettazione e prototipazione di Api, Api Analysis
2. **Persistence & Orchestration Layer:** Rappresenta lo strato di gestione delle interazioni basata su servizi tra i moduli funzionali della soluzione, i moduli che gestiscono il flusso di lavoro ed i moduli funzionali presenti nel resto del sistema informativo di aziendale. È grazie a questo strato che vengono gestiti i flussi di integrazione principali previsti dai profili IHE supportati, nonché alcune integrazioni basate su altri standard, come messaggi HL7. A tal fine, la creazione di “DataLake” garantisce la semplificazione del processo di caricamento e supporta la possibilità di operare su dati (sia strutturati – quali quelli provenienti dal FSE - che non strutturati) e li valorizza prospettandone l’arricchimento informativo ed il riuso.
3. **Portale del cittadino:** Lo strumento principe per la diffusione dei servizi sanitari: accesso al FSE, scelta e revoca dei MMG/PLS, autocertificazione delle esenzioni per reddito. Questo strumento consentirà sia ai cittadini sia agli operatori di settore (ASL, MMG/PLS, Operatori sanitari, …) di accedere ai dati in esso archiviati secondo policy di accesso e protezione delle informazioni che saranno opportunamente definite e concordate con tutti gli attori del processo.

L’architettura complessiva di interoperabilità col Fascicolo Sanitario Elettronico è evidenziata nella seguente figura:

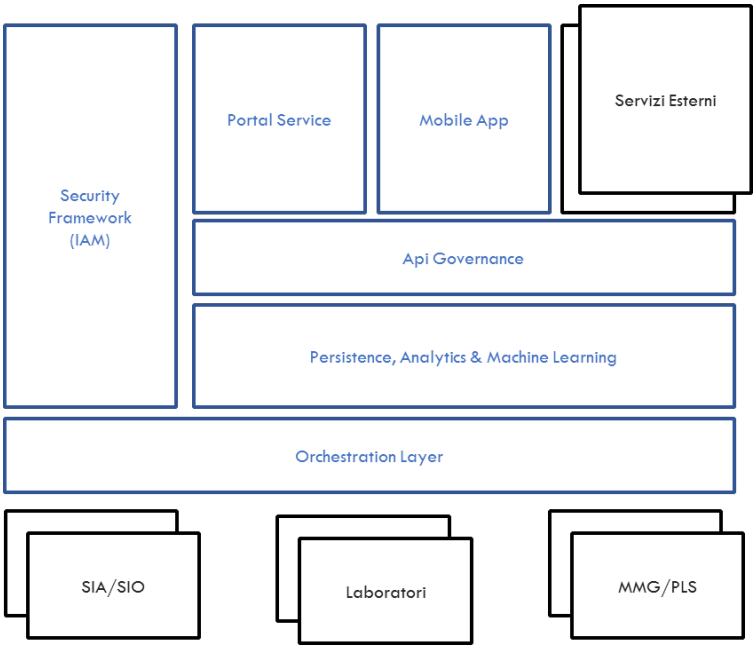

Figura 1 Architettura di alto livello della soluzione

Le componenti logiche della soluzione applicativa di interesse nell’ambito di definizione delle linee guida di Interoperabilità sono le seguenti:

- Api Management;
- Persistence, Analytics & Machine Learning;
- Orchestration Layer.

Le componenti identificate consentono di gestire i flussi previsti per l’interoperabilità del Fascicolo Sanitario Elettronico nelle due componenti relative all’orchestrazione dei servizi ed acquisizione dei dati dai sistemi periferici (Data Ingestion ed Interoperabilità) e alla realizzazione di servizi a valore aggiunto.

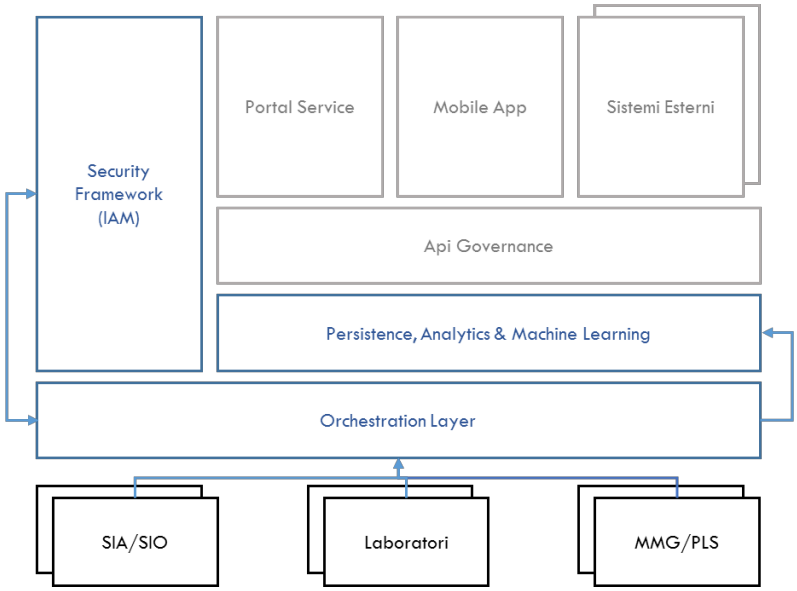

Figura 2 Ingestion dei Dati

L’ingestion dei dati sull’infrastruttura e il colloquio con i sistemi nazionali e centrali verrà realizzato tramite le componenti di orchestrazione, responsabile dell’esposizione dei servizi per i sistemi periferici, il Security Framework per l’autorizzazione degli accessi ai servizi, il layer di Persistenza per la memorizzazione temporanea e indicizzazione dei dati nella cache.

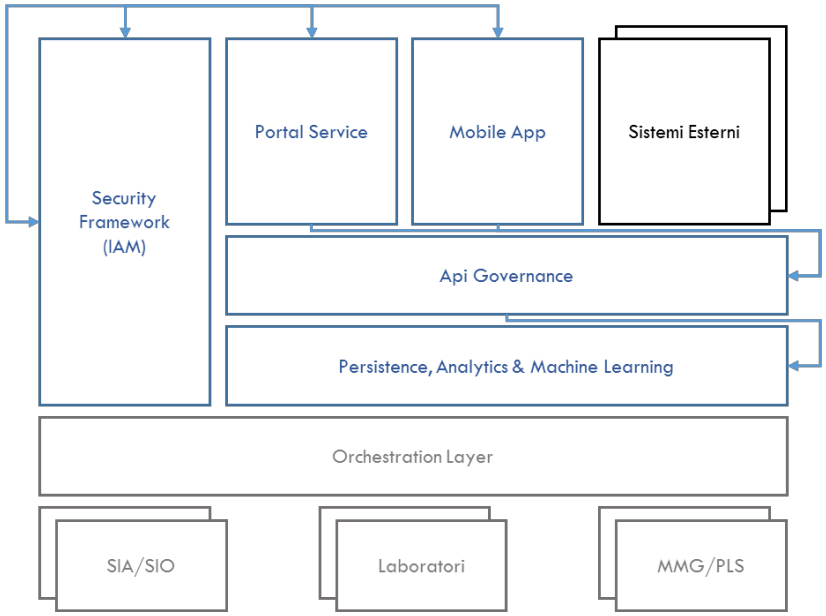

Figura 3 Service Layer

La realizzazione dei servizi a valore aggiunto (Portale del Cittadino, Mobile Apps, etc…) si esplica nelle componenti applicative di Front End, intese come il layer applicativo necessario alla fruizione dei servizi di piattaforma verso gli stakeholders esterni (Cittadino, PMI, etc..).

3.2. API GOVERNANCE & MOBILE FIRST DESIGN

La componente di API Governance è implementata attraverso il prodotto WSO2 API Manager, opportunamente integrato con la componente WSO2 Identity Server.

Le funzionalità fornite dall’API manager sono le seguenti:

- Disegno e prototipazione di API
    - Disegno di API e raccolta di feedback da parte degli sviluppatori prima di renderle operative (API First Design). La progettazione può essere eseguita dall'interfaccia di pubblicazione o importando una definizione Swagger 2.0 esistente
    - Implementazione di API “mock” utilizzando il linguaggio JavaScript
    - Supporto alla pubblicazione di servizi REST e SOAP con codifica JSON o XML
    - Disponibilità di API di esempio precaricate
- Pubblicazione di API e governo del loro uso
    - Pubblicazione di API a consumer e partner esterni, nonché agli utenti interni
    - Possibilità di pubblicare API in un set selezionato di gateway in un ambiente multi-gateway
    - Gestione della visibilità dell'API e limitazione dell’accesso a partner o clienti specifici
    - Gestione del ciclo di vita dell'API: creazione, pubblicazione, sospensione e gestione delle API deprecate
    - Pubblicazione delle chiavi di produzione e sandbox per le API per agevolare il test degli sviluppatori
    - Gestione delle versioni delle API e del loro stato di distribuzione in base alla versione
    - Personalizzazione del ciclo di vita dell'API, compresa un eventuale comportamento personalizzato sulle transizioni del ciclo di vita
- Controllo degli accessi e gestione della sicurezza
    - Convalida il contenuto del payload API in base ad uno schema
    - Applicazione di policy di sicurezza alle API (autenticazione, autorizzazione)
    - Implementazione dello standard OAuth2 per l'accesso alle API
    - Collegamento a server esterni come alternativa a quello “*embedded*” per la registrazione dell'applicazione e la generazione e la convalida dei token Oauth2
    - Blocco di una sottoscrizione e limitazione completa di un'applicazione
    - Possibilità di associare alle API livelli di servizio definiti dal sistema
    - Generazione di JSON token Web a beneficio dei server di back-end
    - Configurazione del Single Sign-On (SSO) utilizzando lo standard SAML 2.0
    - Rilevamento di minacce, di bot e di potenziali frodi nell’uso dei token
- Portale per gli sviluppatori
    - Fornisce una user experience simile agli store di app

- E’ possibile cercare le API per provider, tag o nome
- Possibilità di gestire le chiavi per le API
- Possibilità di sottoscriversi alle API e di gestire le sottoscrizioni delle singole applicazioni
- Possibilità di gestire le sottoscrizioni con diversi livelli di servizio
- Console interattiva per il test di API
- Supporto per l'internazionalizzazione
- Possibilità di ricevere notifiche sulla disponibilità di nuove versioni di API per cui è stata effettuata una sottoscrizione

La piattaforma è stata realizzata mediante la suite WSO2 e nello specifico:

- WSO2 ApiManager
- WSO2 Analitycs
- WSO2 Identity Manager

Tutti prodotti open source con licenza di utilizzo GPL.

Le principali componenti messe a disposizione dalla piattaforma sono rappresentate nella figura seguente:

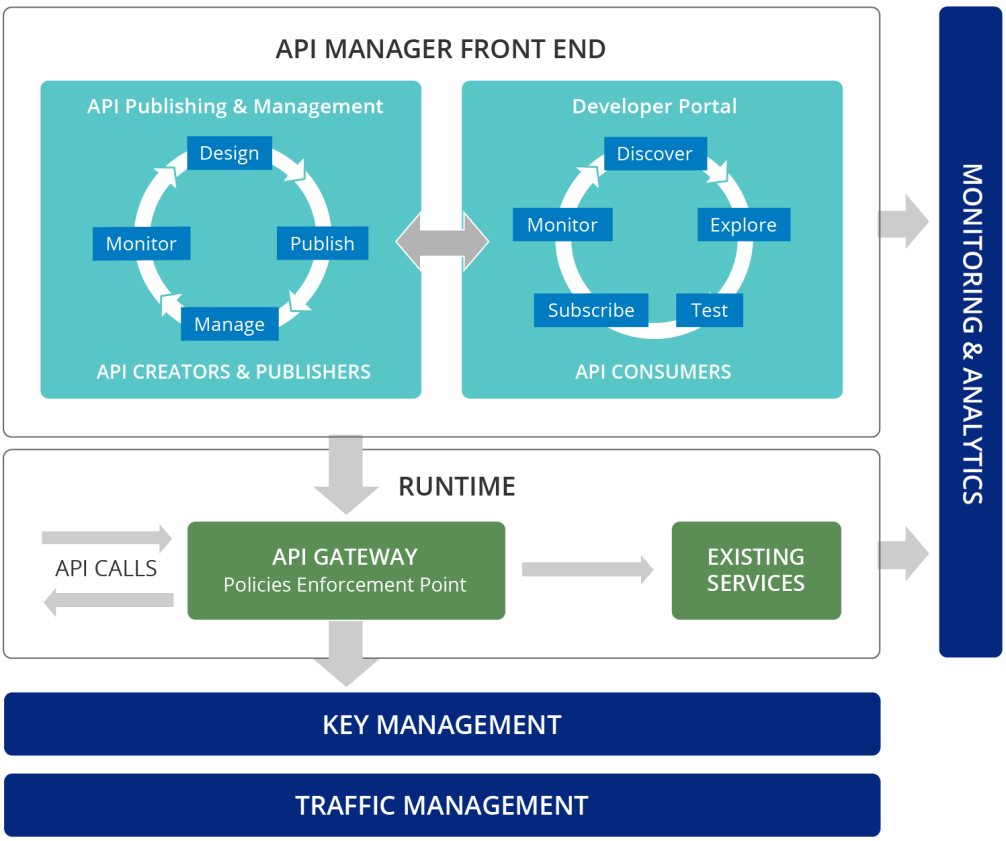

Figura 4 Api Manager

Lo sviluppo di API è generalmente realizzato da risorse in grado di comprenderne gli aspetti tecnici, le loro interfacce, la loro documentazione, le loro versioni, ecc… mente la gestione delle API è tipicamente affidata a qualcuno che ne coglie gli aspetti di business.
In molti contesti lo sviluppo delle API è una responsabilità distinta dalla pubblicazione e dalla gestione delle stesse.

Il prodotto WSO2 API Manager fornisce una semplice User Interface chiamata WSO2 API Publisher che serve a questo scopo. È un front-end progettato per consentire agli sviluppatori di API di censirle, documentarle e versionarle, facilitando al contempo i task relativi alla gestione delle stesse quali la pubblicazione, la monetizzazione, l’analisi delle statistiche e la promozione delle stesse.

La web application di API Store fornisce invece una interfaccia grafica per chi pubblica API che gli consente di censire e pubblicizzare le proprie API, e per i consumatori di API di registrarsi e cercare, valutare e sottoscriversi all’uso di API sicure poiché protette da un sistema di autenticazione.

La componente di API Gateway è una componente di runtime di backend che agisce API proxy ed è sviluppata sulla base di WSO2 ESB. Tale componente rende le API sicure, le protegge, le gestisce e permette di scalare le chiamate alle API. Le richieste alle API vengono intercettate da questo componente che applica le politiche quale il “throttling” (la limitazione della frequenza delle chiamate), la sicurezza (attraverso handlers) e gestisce le statistiche. Se la chiamata soddisfa le policy, il Gateway inoltra la chiamata al corrispondente sistema di backend. Se la chiamata si riferisce ad una richiesta di token, il gateway inoltra la chiamata al Key Manager.

La componente di Key Manager gestisce tutte le operazioni relative alla sicurezza e ai token di accesso. Il gateway si connette al Key Manager per verificare la validità dei token OAuth e delle corrette sottoscrizioni alle API. Quando viene creata un’applicazione e viene generato un token utilizzando l’API Store, questo effettua una chiamata all’API Gateway, che a sua volta si connette al Key Manager per creare un OAuth client ed ottenere un access token. In modo similare, per validare un token, l’API Gateway chiama il Key Manager il quale rintraccia e valida il token dal database.

Il Key Manager fornisce anche una specifica API per generare token OAuth che possono essere acceduti attraverso il gateway. Tutti i token usati per la validazione sono basati sullo standard OAuth 2.0.0. L’API Gateway supporta l’autenticazione con OAuth 2.0 e abilita le organizzazioni a imporre un limite nella frequenza delle chiamate.

Il Key Manager disaccoppia le operazioni per la creazione di applicazioni OAuth e di validazione degli access token rendendo possibile la delega del processo di validazione delle chiavi a sistemi terzi.

La componente di Traffic Manager aiuta gli utenti a regolare il traffico delle API, rendendo possibile la differenziazione dei livelli di servizio tra diversi consumer, prevenendo in questo modo anche possibili attacchi di sicurezza. Sostanzialmente il Traffic Manager lavora come un engine dinamico per le politiche di throttling in real-time, inclusa la limitazione del rating delle richieste alle API.

La componente di WSO2 API Manager Analytics fornisce capabilities di monitoraggio e analisi in grado di fornire statistiche in forma grafica ed analitica, meccanismi di alerting su eventi pre-determinati e di analisi dei log.

3.2.1. API GATEWAY

L’API Gateway, cuore della soluzione, ha come finalità essenziale quella di esporre i servizi messi a disposizione dall’intero sistema in maniera sicura, facilmente fruibile e controllata.

Esso si posiziona davanti ai servizi esposti dal backend, in modo tale che tutti i sistemi esterni debbano effettuare l’accesso a servizi e risorse attraverso questo componente. Infatti, il Gateway, per ogni accesso al sistema da parte di un’applicazione esterna, effettua i seguenti passi:

- Riceve le richieste per accedere alle API
- Attua le politiche di controllo di accessi, integrandosi se necessario anche con altre componenti
- Applica le regole di rate limiting e throttling
- Invia le richieste al backend dell’API (questo step può essere mediato dall’ESB)
- Effettua il routing della risposta al sistema chiamante.

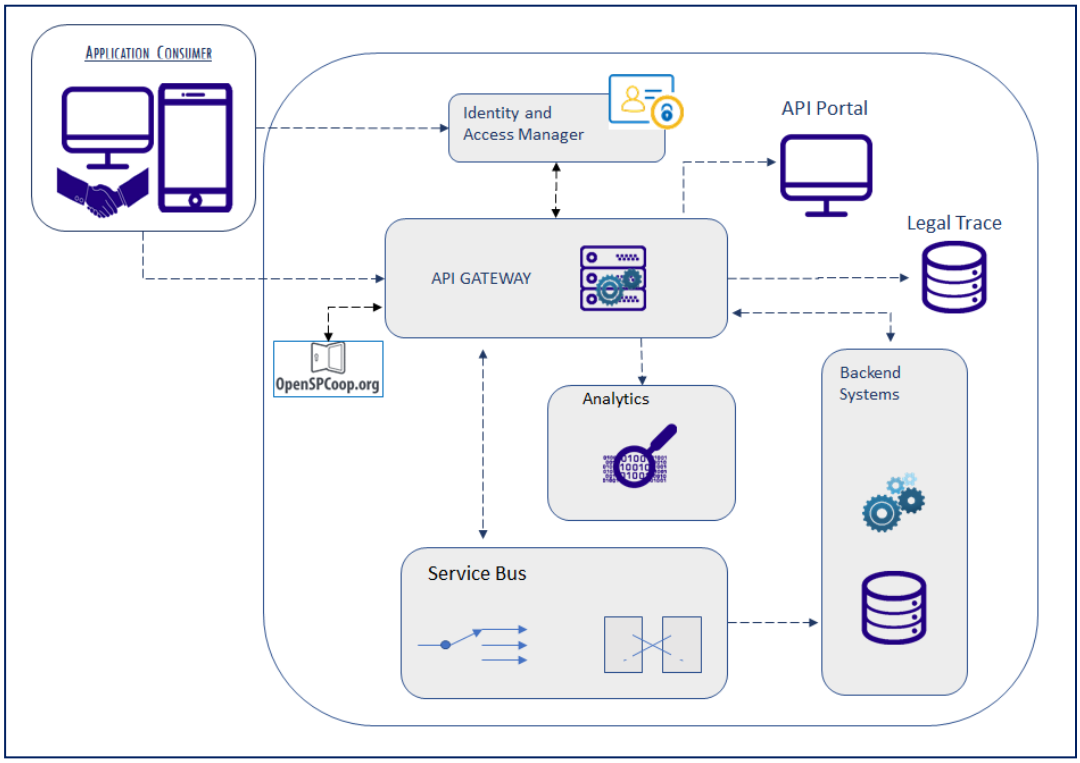

Figura 5 Api Gateway

Gli obiettivi principali di tale sistema possono essere riassunti come segue:

- Livello di sicurezza: garantisce l’accesso soltanto agli utenti/sistemi autenticati e autorizzati ed evita l’uso improprio delle risorse protette. Sono disponibili diversi framework di sicurezza come OPENID, OAuth2, SAML o Basic Authentication che consentono a diverse applicazioni di integrarsi in modo sicuro dipendentemente dallo scenario e dalle esigenze implementative. (in integrazione con il componente Key Manager)
- Performance gestite in maniera puntuale e dinamica per ciascuna API con
    - Limitazione del traffico in ingresso (rate limiting)
    - Applicazione di politiche di accesso diversificate in base sistema chiamante (throttling)

  - Routing
  - Mediazione dei servizi
  - Caching dei messaggi
- Filtraggio del traffico in ottica di identificazione e neutralizzazione di minacce
- Gestione del ciclo di vita delle API nelle fasi di sviluppo, test, produzione e dismissione, nonché versionamento. Questa funzionalità garantisce la coerenza di differenti versioni dell’API consentendo il suo utilizzo da parte di diverse tipologie di utenti, in ambienti diversi e con diversi gradi di maturità
- Monitoring e alerting configurabili per verificare lo stato del sistema ed alimentare sistemi di notifica nel caso in cui si verifichino eventi inattesi (in integrazione con il sistema di Analytics)
- Flessibilità nei protocolli: supporto di servizi di backend di tipo Web Service o REST e possibilità di esporre tali servizi modificandone il protocollo. Questo consente di esporre anche servizi pre-esistenti in nuove modalità senza la necessità di cambiare l’implementazione del servizio stesso
- Esposizione della API in diverse modalità: di particolare interesse sono le API Rest e Web Socket
- REST: I servizi che si conformano allo stile REST (REpresentational State Transfer) espongono interfacce che consentono di manipolare le risorse applicative offerte dal servizio attraverso l’utilizzo uniforme di un set di operazioni. I servizi REST rispondono alle richieste inviate dai consumer ritornando opportune rappresentazioni delle risorse, e non conservano alcuno stato circa le interazioni avvenute. Le risorse sono univocamente determinate dall’URI e, ove necessario, modificate tramite query parameters e payload delle request, solitamente in formato JSON
- Web Socket: Le API esposte come websocket forniscono una comunicazione bidirezionale in tempo reale applicabile a qualunque tipo di applicazione client-server. Permette maggiore interazione tra un client e un server, facilitando la realizzazione di applicazioni che forniscono contenuti in tempo reale. Questo è reso possibile fornendo un modo standard per il server di mandare contenuti al client senza dover essere sollecitato dal client e permettendo ai messaggi di andare e venire tenendo la connessione aperta.

3.2.2. KEY MANAGER

Il Key Manager, chiamato anche Authorization Server, in integrazione con l’API Gateway, è il componente deputato alla gestione degli accessi e all’autorizzazione delle richieste attraverso l’utilizzo di diversi protocolli di autenticazione e autorizzazione quali OPENID, SAML, OAuth2, Basic Authentication.

3.2.2.1. FRAMEWORK OAUTH2

Tra gli standard messi a disposizione, Open Authorization 2 (OAuth2) è quello che ha avuto una maggiore affermazione nell’esposizione delle API; esso costituisce un framework di comunicazione open mediante il quale si può gestire in modo sicuro l’accesso autorizzato a risorse protette.

Al contrario degli approcci tradizionali, offre i seguenti vantaggi:

- Le applicazioni non devono memorizzare in nessuna forma le credenziali degli utenti
- Le risorse vengono fornite alle applicazioni in modo controllato sia in termini di scope che in termini temporali
- L’utente finale può revocare l’accesso alle proprie risorse limitatamente a determinate applicazioni, senza la necessità di dover cambiare le credenziali
- La scelta implementativa non è univoca, ma si adatta ai diversi scenari di applicazione; per esempio lo standard si differenzia in base alla possibilità dei fruitori delle risorse di mantenere dati in modo sicuro, alla tecnologia impiegata, etc.

Per delineare il funzionamento di OAuth2, si possono definire i seguenti attori:

- Resource Owner: (RO) è il proprietario della risorsa da proteggere.
- Resource Server: (RS) è il server che espone la risorsa protetta, nel nostro caso si tratta dell’API Gateway che si frappone tra Client e servizio di backend. Riceve le richieste da un client che si identifica tramite la presentazione di un access_token e fornisce la risorsa richiesta
- Client: è l’applicazione fruitrice della risorsa. Le applicazioni possono essere di qualsiasi tipo: web, client/server, mobile, desktop
- Authorization Server: (o Key Manager) è il server che, a fronte di una grant del RO, fornisce al client gli access token da presentare al RS per accedere alla risorsa.

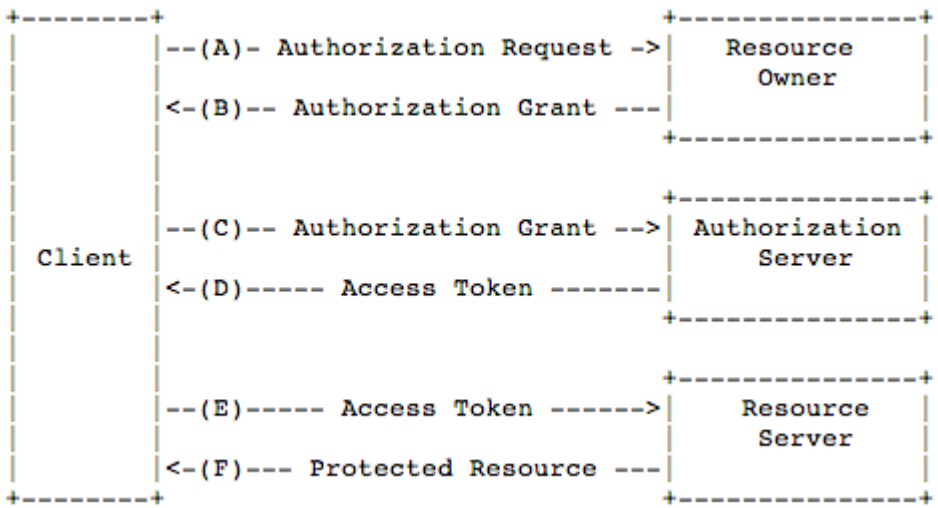

Figura 6- Flusso OAuth2

Il flusso sopra illustrato è il flusso logico che il framework si propone di realizzare. Tuttavia, l’implementazione effettiva dipende dalla natura dei client, dal livello di trust tra resource owner e client e dalle esigenze di tracciatura di accessi e risorse accedute. Si illustrano di seguito i 4 modelli implementativi (grant type):

- Authorization Code
- Implicit
- Onwer Credentials
- Client Credentials

Per le esigenze espresse nel progetto, il flusso da prendere in considerazione è il Client Credentials poiché esso prevede un’interazione server to server e non necessita della partecipazione dell’utente finale nell’accesso alle risorse protette, ma è il client stesso che, essendo trusted, può effettuare l’accesso alle API.

Questo flusso prevede che il client si sia precedentemente registrato sull’Authorization Server e che gli siano stati associati Client ID e Client Secret. Tali dati vengono memorizzati staticamente nel Client ed utilizzati a runtime per richiedere l’Access Token. Pertanto, il client deve essere in grado di salvare in modo sicuro le credenziali, tipicamente in scenari server to server.

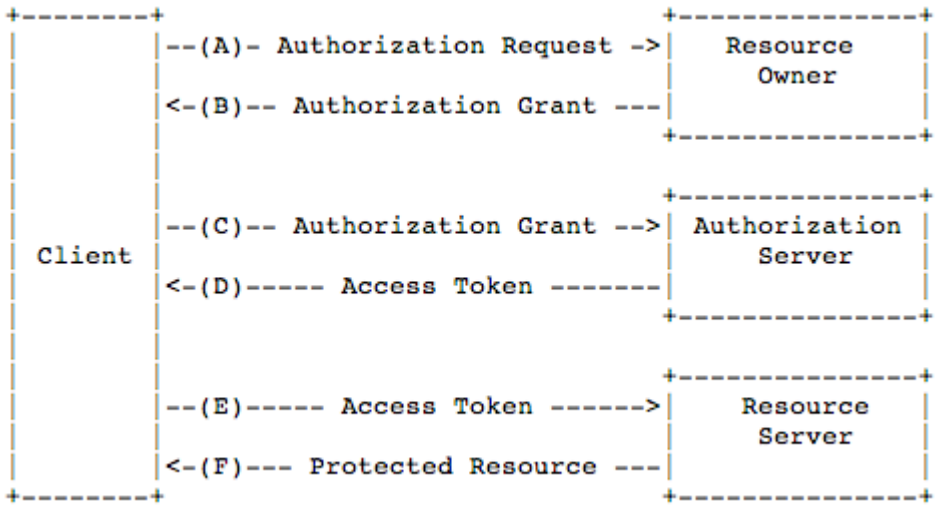

Figura 7 - OAuth2 Client Credentials

Come conseguenza, il flusso Client Credentialsviiene utilizzato nei casi in cui:

- Le risorse oggetto dell’autorizzazione sono limitate alle risorse protette sotto controllo del client
- Le risorse sono state precedentemente concordate con l’Authorization Server (forte TRUST sul Client)
- Il Client coincide con il Resource Owner
- Viene utilizzato quando NON c’è esigenza di tracciare l’utilizzatore finale

Ottenuto l’Access Token, il Client può contattare il Resource Server per richiedere le risorse. Allo scadere dell'access token, il client dovrà richiederne uno nuovo seguendo lo stesso approccio.

3.2.3. IDENTITY SERVER

La soluzione prevede l’utilizzo di un Identity Server (IS) che unifichi la gestione delle utenze e dei gruppi in maniera cross su tutte le componenti.

Oltre che a garantire un single sign-on su tutti i sistemi e la federazione con altri Identity Provider, l’Identity Server viene utilizzato come Identity Provider nei flussi autorizzativi OAuth2 fornendo la parte di autenticazione ed affiancandosi al Key Manager che fornisce invece la parte autorizzativa.

L’Identity Server (IS) fornisce una gestione sicura delle utenze, gestendo identità e ruoli in modo centralizzato, con la possibilità di federare altri Identity Server in modelli n-n o 1-n. Nel primo caso i consumer possono interfacciarsi con un unico Identity Provider federato e centralizzato, nel secondo caso, invece, i consumer possono interfacciarsi con n Identity Provider in modo che sia garantita la massima flessibilità.

Le funzionalità messe a disposizione dall’Identity Server sono molteplici:

- Gestione accessi:
  - Supporto XACML - eXtensible Access Control Markup Language: linguaggio basato su XML per gestire gli accessi in modo puntuale e dettagliata
  - Supporto RBAC - Role Based Access Control: controllo basato sui ruoli degli utenti
  - Supporto ABAC - Attribute Based Access Contro: controllo basato su policy che utilizzano combinazioni di attributi dell’utente
- Sicurezza delle API:
  - OAuth: standard utilizzato per l’autorizzazione che consente ai client di accedere alle risorse del server previa autorizzazione del proprietario della risorsa
- Provisioning:
  - L’IS fornisce API che supportano la creazione degli utenti protette con Basic Authentication e OAuth2
  - Just-in-time (JIT) provisioning: quando l’utente è accreditato presso Identity Providers esterni federati, l’IS ridireziona la richiesta di autenticazione su tali IP, nel momento in cui riceve la risposta positiva, se il JIT provisioning è abilitato, l’utente e i suoi claim vengono memorizzati nello store interno.
  - Outbound Provisioning: l’IS supporta il provisioning delle utenze ad Identity Provider esterni in tutti i flussi iniziati da un Service Provider. Il provisioning va abilitato e si applica a SCIM, SPML, SOAP, Google Apps provisioning API, Salesforce provisioning API.

3.2.4. PUBLISHER PORTAL

Lo sviluppo e la pubblicazione delle API sono permessi da un’interfaccia web messa a disposizione dall’API Manager chiamata Publisher. Si possono raggruppare le funzionalità che l’API Publisher mette a disposizione in 4 macrofunzionalità:

- Sviluppo
- Pubblicazione
- Gestione
- Monitoraggio

La creazione di un API è il processo tramite il quale si collega l'implementazione backend di un servizio con l'API Publisher in modo da gestirne e monitorarne il ciclo di vita, la documentazione, la sicurezza e le varie sottoscrizioni.

Una volta terminata la creazione, l'API può essere pubblicata. Nel momento in cui un API viene pubblicata diventa visibile e disponibile per essere sottoscritta, secondo le configurazioni di visibilità pre-definite.

Le API create nell'API Manager hanno un proprio ciclo di vita formato un insieme di stati. Un'API ha un ciclo di vita definito dall’API Manager. Un esempio di ciclo di vita è quello riportato in figura e composto da 6 stati (Creata, Pubblicata, Bloccata, Deprecata, Prototipata e Dismessa) ma diversi modelli possono essere realizzati.

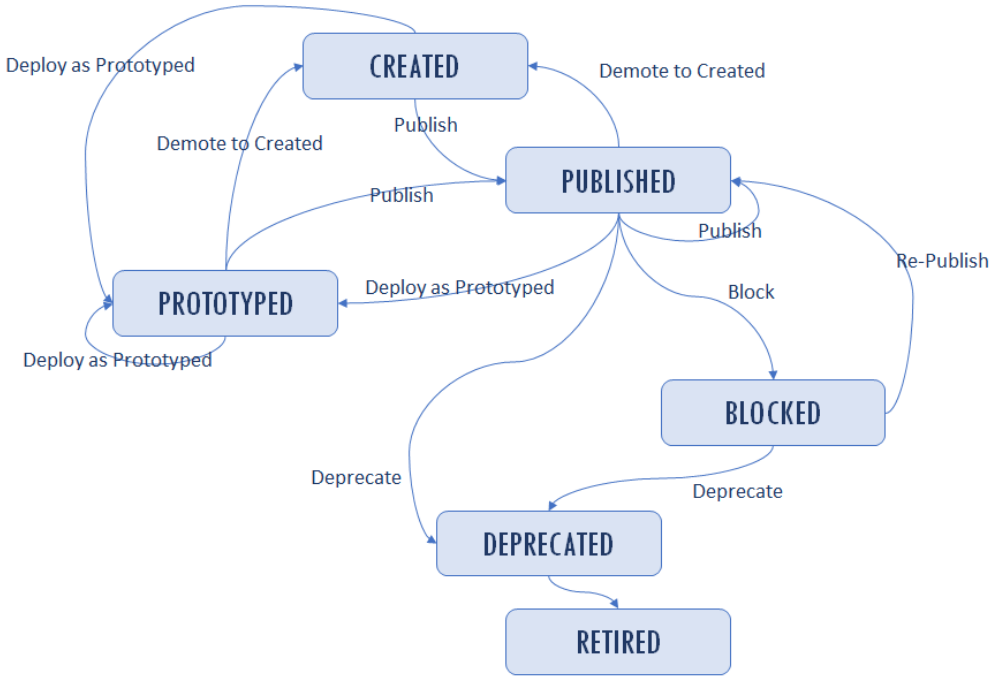

Figura 8 - Ciclo di vita dell'API

È possibile, inoltre, creare differenti versioni di un API, quando, ad esempio, si modificano alcune funzionalità dell'API stessa o quando cambiano i meccanismi di autenticazione o livelli di throttling.

Una funzionalità molto importante durante lo sviluppo di un API è la possibilità di aggiungere la documentazione del servizio offerto per facilitare da una parte i sottoscrittori a capirne le funzionalità, dall'altra i publisher per promuoverla.

3.2.5. STORE PORTAL

Qualunque ente voglia accedere ai servizi, dovrà effettuare preventivamente un accreditamento presso l’entità erogante. Questa sarà un’attività di tipo procedurale che prevede:

- Accordi bilaterali sull’utilizzo delle API esposte
- Accordi sul livello di servizio
- Accordi sulle politiche di rate limiting e client throttling per l’utilizzo
- Creazione di utenze tecniche per accedere ai servizi offerti
- A valle dell’espletamento di tale procedura, l’utenza tecnica creata potrà essere utilizzata per accedere al portale API Store.

Il portale è uno strumento a disposizione degli sviluppatori, che fornisce funzionalità utili al discovery delle API esistenti e al loro utilizzo.

- Navigazione delle API alle quali l’operatore si può sottoscrivere
- Versionamento delle API
- Consultazione della documentazione associata alle API
- Generazione automatica di codice per invocare le API

I consumers (siano essi App esterne o sviluppatori) hanno la possibilità di navigare nello Store per ricercare quelle di loro interesse, potendo sfruttare anche i commenti e le valutazioni degli altri utenti presenti nei forum interni. Le ricerche possono essere effettuate per nome, service provider, descrizione, stato.

È importante sottolineare che NON tutte le API sono pubbliche; esistono, infatti diversi livelli di visibilità:

- Pubblico: l'API è visibile a tutti gli utenti (registrati e anonimi).
- Visibile nel dominio: l'API è visibile a tutti gli utenti registrati nel dominio dell'API.
- Restrizione per ruolo: l'API è visibile solo a utenti specifici.

Per poter utilizzare un API bisogna, prima di tutto, creare un'applicazione mediante la quale effettuare la sottoscrizione. Il ruolo principale dell'applicazione è disaccoppiare il consumer dalle APIs e permette sia di generare e utilizzare una chiave singola per più API che di sottoscriversi più volte ad una singola API con diversi livelli SLA.

Le applicazioni sono disponibili a diversi livelli di servizio che corrispondono al numero massimo di chiamate che è possibile fare a un'API durante un determinato periodo di tempo (throttling). Questo meccanismo risulta utile quando sono presenti limitazioni dell'infrastruttura per fare in modo che l'applicazione possa effettuare un numero massimo di richieste entro un tempo definito.

La sottoscrizione ad un API consente di richiedere a runtime il token di accesso, una stringa semplice che viene passata nell'intestazione HTTP di una richiesta per autenticare gli utenti e garantire alti livelli di protezione. Se un token passato con una richiesta non è valido, la richiesta viene eliminata nella prima fase di elaborazione.

3.3. ORCHESTRATION LAYER & ANALYTICS

La piattaforma di interoperabilità deve, tra le altre cose, prevedere la possibilità di poter integrare eventuali altre soluzioni e tecnologie di dominio di un soggetto aderente alla piattaforma. Considerando l’insieme delle tecnologie previste per lo scambio di informazioni, l’eterogeneità dei protocolli di comunicazione previsti, la flessibilità di dislocazione dei servizi che saranno esposti e fruiti, si è prevista l’introduzione di un “Integration Layer”.

L’Integration Bus è la componente software che abilita la comunicazione tra le diverse componenti della piattaforma e i sistemi esterni attraverso una moltitudine di protocolli e formati di messaggio. Oltre a ricoprire un aspetto fondamentale nell’abilitazione del trasporto di messaggi con svariate tipologie di protocolli nonché la conversione da un protocollo all’altro all’interno di una stessa comunicazione, il Service Bus permette di integrare applicazioni eterogenee evitando la connessione diretta tra le stesse, disaccoppiando e scongiurando potenziali modifiche che potrebbero arrecare impatti anche consistenti sulle caratteristiche delle stesse.

Le caratteristiche principali del Service Bus sono la versatilità, la velocità e la flessibilità; adottando i principi degli Enterprise Integration Patterns permette di realizzare una grande quantità di scenari di integrazione fra componenti.

Di seguito una raffigurazione delle logiche applicative oggetto di esame:

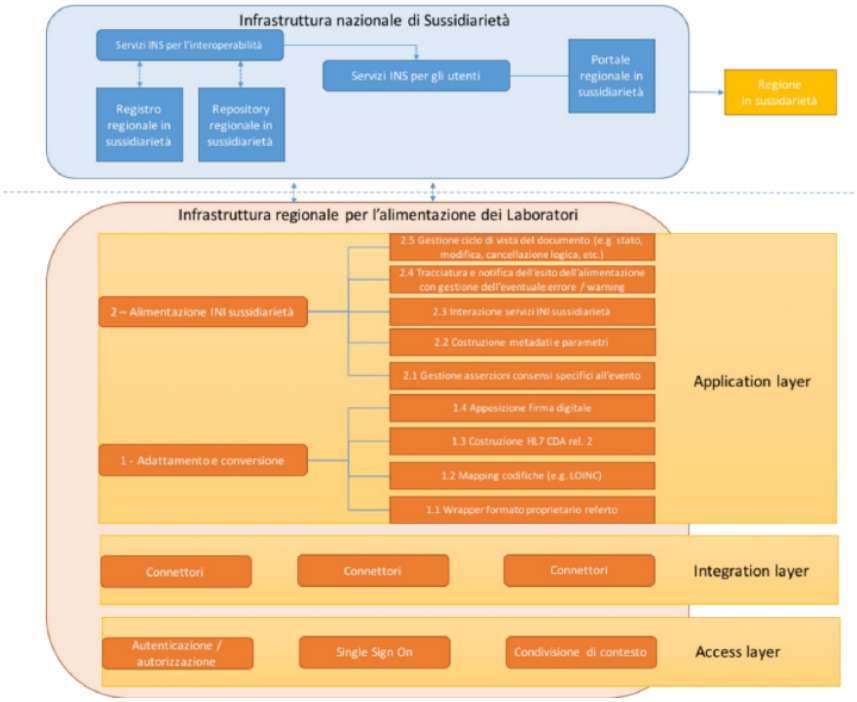

Figura 9 Vista funzionale

Secondo le indicazioni di SOGEI, la piattaforma di cooperazione potrà prevedere alla indicizzazione preventiva della documentazione anche in assenza del Consenso. Si citano testualmente le indicazioni ITI FSE di SOGEI:

[…] L'indicizzazione di documenti sanitari può essere realizzata anche senza l'esplicito consenso rilasciato dall'assistito, in modo da consentire all'atto dell'istituzione del FSE la possibilità di recuperare il pregresso clinico dell'assistito. Tale processo di indicizzazione preventiva deve però assicurare che i documenti non confluiscano nel FSE (ovvero che i documenti non possono essere ricercati e consultati attraverso il FSE) […]

Nel caso specifico della Regione Campania, dato che i componenti di Consenso e di Visualizzatore per il cittadino saranno proprio quelli forniti da SOGEI, si prevedono tutte le attività necessarie per l'indicizzazione e il relativo flusso documentale verso FSE ITI.

Il flusso procedurale prevede la raccolta e trasformazione dei flussi, mediante utilizzo di appositi canali esposti dalla Piattaforma di cooperazione applicativa, e l'alimentazione mediante appositi servizi forniti dal sistema INI-FSE del FSE di interesse, secondo le specifiche tecniche pubblicate dal decreto MEF del 4 agosto 2017.

L'infrastruttura della Piattaforma di Cooperazione posta in essere si comporrà di moduli e interfacce efficaci in grado di combinarsi, sulla base delle strategie di integrazione e allineamento tra software LIS e sistema cooperativistico, con il FSE-INI.

La flessibilità e potenzialità dell'infrastruttura oggetto di proposta, è funzione delle logiche funzionali demandate a tre livelli applicativi a loro volta in grado di dialogare a valle con il sistema sanitario regionale e con i suoi nodi, ed a monte, di esporre viste strutturate all'Infrastruttura Nazionale di Sussidiarietà.

Il modello architetturale funzionale prevede cinque layer:

- **Access Layer**: rappresenta il punto di accesso alla soluzione. Attraverso questo layer, utenti e amministratori della piattaforma potranno accedere ai diversi moduli, per fruire delle funzionalità offerte.
- **Application Layer**: rappresenta lo strato in cui sono collocate le Applicazioni, contenenti la logica di business del sistema e fruibili mediante un'architettura orientata ai servizi. Per alcuni di questi servizi è disponibile, in aggiunta all'accesso attraverso la logica SOA, l'esperienza d'uso mediante un'interfaccia utente semplice e intuitiva. Le applicazioni sono utilizzabili da parte di tutti i soggetti interessati a conoscerne, testarne e utilizzarne i servizi e le API.
- **Business Process Layer**: rappresenta l'area funzionale i cui moduli governano la costituzione e l'avanzamento dei processi di lavoro, siano essi di natura clinico-diagnostica, sanitaria, amministrativa o di controllo direzionale.
- **Integration Layer**: rappresenta lo strato di gestione delle interazioni basata su servizi tra i moduli funzionali della soluzione, i moduli che gestiscono il flusso di lavoro ed i moduli funzionali presenti nel resto del sistema informativo di aziendale. È grazie a questo strato che vengono gestiti i flussi di integrazione principali previsti dai profili IHE supportati, nonché alcune integrazioni basate su altri standard, come messaggi HL7. Alla gestione mediata dai moduli funzionali di integration layer si affianca una interazione diretta tra i moduli del layer application prevista in alcuni scenari per sostenere le esigenze di efficienza prestazionale e flessibilità di interazione.

- **Data Layer**: rappresenta l’impianto di gestione dei dati. A questo livello si situano tutti i moduli che garantiscono la persistenza dei dati e dei documenti nel tempo, nonché la loro catalogazione ed indicizzazione per i documenti che non vengono storicizzati da FSE-INI. A questi si affiancano i moduli di gestione dei dati di configurazione e di natura amministrativa.

A ciascuno dei cinque livelli dell’architettura funzionale sono associati i moduli funzionali facenti parte dell’architettura, che indirizzano i business requirements grazie al contributo preminente di componenti applicative distribuite a quello stesso livello. Questa associazione tra layer e moduli consente di comprendere quali siano le responsabilità ed il valore aggiunto, in termini funzionali, di ciascun livello, nonché di stabilire una denominazione comune per i diversi insiemi logici di funzionalità.

La descrizione architetturale prosegue poi presentando un modello di distribuzione, nel quale i moduli funzionali sono distribuiti sul territorio secondo criteri atti a garantire:

- Efficienza prestazionale: privilegiando la distribuzione sui nodi territoriali di tutte le componenti mission-critical per gli operatori sanitari
- Robustezza della soluzione: distribuendo sul territorio di alcuni moduli che assumono un ruolo di importanza strategica per la garanzia di continuità di servizio applicativa
- Ampia accessibilità ai servizi: scegliendo di centralizzare i moduli che consentono l’accesso agli indici ed ai documenti e dati su scala regionale, così da renderli di fruibili in modo equivalente da parte di tutte le aziende sanitarie
- Conformità alla normativa: mantenendo nella sfera di competenza della singola Azienda Sanitaria la completa gestione delle informazioni sulla privacy nonché la titolarità dei documenti clinici
- Centralizzazione: mantenendo un elevato livello di centralizzazione nel governo dei servizi esposti, garantendo al contempo un equilibrio efficiente dal punto di vista di manutenibilità, flessibilità e apertura rispetto ad eventuali evoluzioni future del sistema ed alle interazioni tra l’azienda sanitaria ed il territorio

I Layer Access Control, Business Process, Integration Platform, e Data Repository sono la trasposizione a livello applicativo dei layer al medesimo livello nell’architettura funzionale, di fatto traducendo in moduli applicativi i moduli funzionali li descritti. I Layer User Interface e Services sono invece frutto della scomposizione del layer funzionale “Application”: a livello di architettura applicativa vengono infatte distinti i moduli di più alto livello, che erogano funzionalità mediante interfacce utente, da quelli di più basso livello che erogano servizi.

3.3.1. ARCHITETTURA FUNZIONALE

La relazione tra livelli architetturali e moduli funzionali, dato l’elevato numero di moduli presenti, è rappresentata in una serie di diagrammi. Il primo di questi ha il compito di inquadrare l’architettura a livello generale ed introdurre le funzionalità comuni all’intera soluzione, mentre i seguenti approfondiscono l’architettura di ciascuno dei sistemi oggetto di fornitura, presentandone i moduli funzionali specifici. L’architettura funzionale generale è schematizzata nel seguente diagramma:

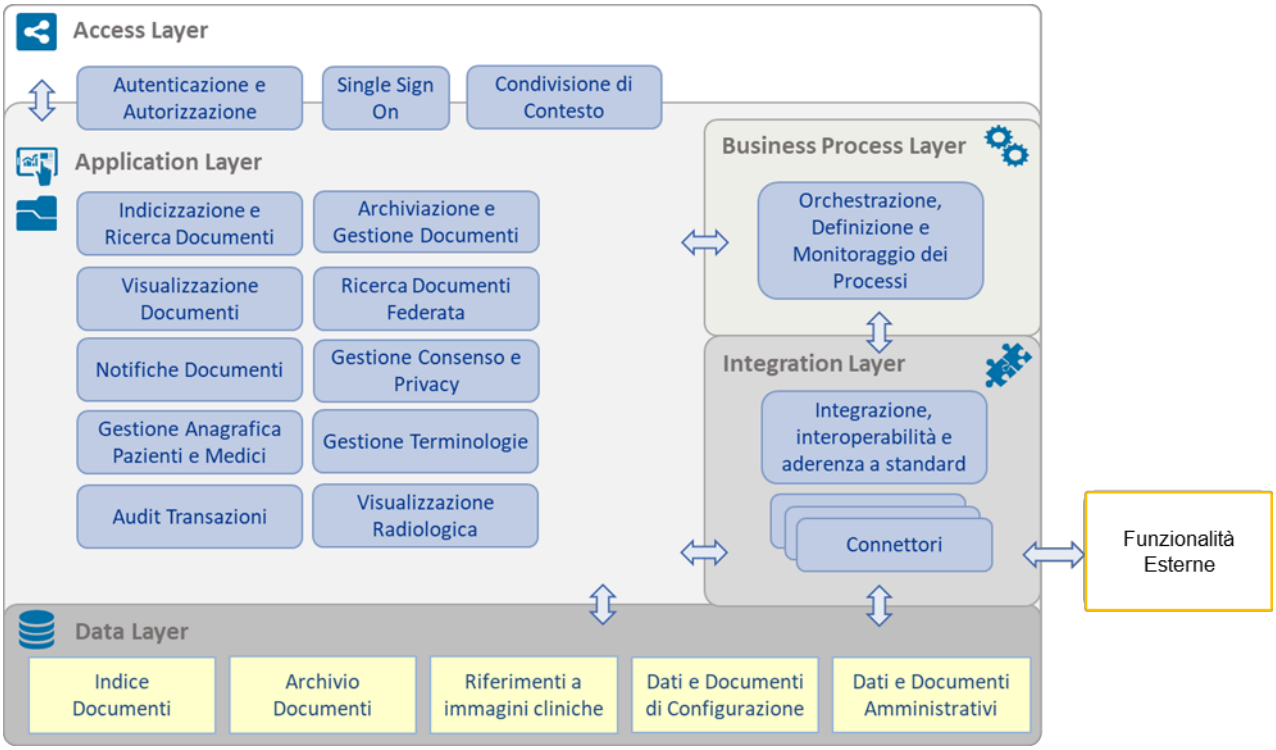

Figura 10 Architettura Funzionale

Il sistema proposto adotta soluzioni atte ad impedire l’alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali. Il livello Access Layer garantisce un accesso sicuro a tutti i moduli funzionali del sottostante livello “Application”, il quale offre funzionalità fruibili mediante interfaccia grafica o servizi. I moduli del livello Application interagiscono tra loro secondo servizi basati sull’implementazione di profili IHE o attraverso API native: l’elevato numero di interazioni tra i moduli, non rappresentato nel diagramma.

I moduli del livello Application interagiscono con logica bidirezionale con il modulo di “Orchestrazione, definizione e monitoraggio dei processi”, sfruttandolo per la gestione del flusso di lavoro, nonché con il modulo “Integrazione, Interoperabilità e aderenza a Standard” grazie al quale possono attivare i flussi di integra-zione con il resto del sistema informativo.

All’interno dell’architettura sono distribuiti i seguenti moduli funzionali:

Autenticazione e autorizzazione

La soluzione proposta in fornitura pone particolare attenzione al trattamento dei dati sensibili

garantendo un elevato grado di riservatezza e di sicurezza come previsto dalle norme sulla privacy - D.Lgs. 196/03 e successive integrazioni - ed anche in relazione all'articolo 22 comma 6 del decreto stesso per il quale è stata adottata la tecnica di separazione dei dati anagrafici dai dati sanitari tramite l'utilizzo di codici identificativi. La soluzione è conforme alla normativa vigente,

anche rispetto alle recenti emanazioni del Garante in merito al tracciamento degli accessi degli amministratori.

Sono previste funzioni ed utilità ad uso amministrativo di sistema volte ad agevolare la gestione operativa ed il controllo del rispetto delle normative:

- i sistemi consentono un accesso tramite credenziali assegnate ad ogni singolo utente e verificate tramite l’Identity Provider di sistema;
- gestire il ciclo di vita (creazione, modifica, sospensione e cancellazione) degli account; esporre funzioni preposte al controllo, revoca e modifica dei diritti d’accesso agli oggetti e alle funzionalità degli applicativi;
- Assegnare credenziali in modo univoco con la possibilità di rilascio e revoca dei diritti di accesso agli account nelle situazioni di urgenza/emergenza;
- configurare un tempo limite oltre il quale le credenziali inutilizzate vengono automaticamente disattivate;
- l’utente può modificare la propria password autonomamente in qualsiasi momento; configurare il tempo dopo il quale è necessaria la modifica della password, ed è possibile forzare il cambiamento password in seguito al primo accesso;
- identificare la persona assegnataria delle credenziali per impedirne il riutilizzo delle medesime;
- gestire policies di accesso e visibilità sui contenuti degli utenti abilitati;
- sono previsti profili di accesso ai dati ed alle funzionalità rese disponibili per singoli utenti o a gruppi di essi.

Gli accessi ai servizi di piattaforma e tutte le operazioni effettuate dagli utenti, ad esempio login e consultazioni, sono tracciati e registrati in appositi log di sistema.

La piattaforma inoltre fa uso di tecnologie di crittografia a protezione delle informazioni scambiate come previsto dalle norme vigenti per i sistemi che trattano dati sensibili. In particolare per la comunicazione tra browser e server viene usato il tunneling SSL del protocollo HTTP (HTTPS).

Il modulo di Autenticazione e autorizzazione sovrintende e governa il processo di autenticazione di tutti gli operatori che intendono avvalersi di servizi esposti da altri moduli secondo i criteri descritti poc’anzi, consentendo la gestione sicura dell’intero ciclo di vita delle identità digitali.

Attingendo le proprie informazioni dall’archivio di credenziali eventualmente reso disponibile dall’azienda o basandosi sul proprio LDAP, è in grado di garantire un accesso sicuro e accordare privilegi a seconda del ruolo a tutti gli operatori.

La nostra soluzione di autenticazione e autorizzazione consente la gestione sicura dell’intero ciclo di vita delle identità digitali.

Le principali funzioni offerte sono:

- Integrazione con il repository dell’Anagrafe utenti, organizzata sull’architettura preesistente dell’Azienda;

- Gestione delle identità che include, oltre alle funzionalità standard di Identity Management, anche la capacità di sincronizzazione delle identità detenute dal servizio verso le applicazioni del dominio;
- Gestione centralizzata dei profili autorizzativi e dei ruoli/privilegi associati a ciascun utente;
- Tracciatura e auditing delle operazioni, che include la registrazione degli eventi centralizzata ed adeguate funzioni di aggregazione del dato attraverso sistemi evoluti di ricerca e relativo reporting assicurando la tracciabilità di tutte le registrazioni informatiche effettuate.
- La componente di Audit è basata sull'implementazione del profilo IHE ATNA e implementa anche le funzionalità ATNA RESTful Query che permette ad utenti autorizzati di accedere mediante semplici servizi REST alle informazioni sugli eventi.

La componente di sicurezza viene garantita dall'utilizzo di strumenti di autenticazione basati su standard internazionali (LoA2 – user / pwd -, LoA3 – OTP - e LoA4 – certificati digitali e SAML 2.0).

Tali standard consentono l'intercambiabilità delle componenti, rendendo la soluzione portabile su architetture conformi allo SPID, senza la necessità di dover cambiare il sistema di gestione degli accessi per rispondere alle esigenze di integrazione con altri sistemi regionali o nazionali.

Indicizzazione e Ricerca Documenti

Rende disponibili le componenti funzionali che implementano il profilo IHE XDS per l'attore Registry, consentendo l'indicizzazione dei documenti, la loro catalogazione secondo una serie di metadati definita in un *affinity domain* e la loro ricerca secondo una serie di possibili parametri.

Archiviazione e Gestione Documenti

Implementa il profilo IHE XDS.b per l'attore Repository, consentendo di memorizzare documenti (non di dominio FSE-INI) e riferimenti andando poi ad indicizzarli sul modulo di Indicizzazione e Ricerca Documenti.

Visualizzazione Documenti

Espone le componenti funzionali necessarie ad offrire agli operatori una interfaccia utente di consultazione dei documenti indicizzati sul registry centrale. Il modulo aderisce ai requisiti previsti da IHE per l'attore XDS Consumer

Ricerca Documenti Federata

Il valore garantito dall'uso di uno standard internazionale come IHE XDS per l'interoperabilità documentale è ulteriormente amplificato affiancandovi questo modulo di gestione federata di registry multipli, basato sui profili IHE XCA e XCA-I. Inoltre, grazie all'uso di query federate è possibile accedere da subito ai documenti di tipo non radiologico già oggi indicizzati su

infrastrutture XDS esistenti dotate di registry, dando immediatamente valore aggiunto agli operatori interessati alle informazioni cliniche disponibili sul paziente.

Notifiche documenti

Grazie alle funzionalità garantite da questo modulo, è possibile sfruttare il Registry XDS come punto di riferimento per l'attivazione di workflow che nascono a valle della pubblicazione di un documento. Basato sul profilo IHE DSUB, consente ad altri moduli funzionali di sottoscrivere un invio di notifiche secondo un insieme di criteri relativi ai nuovi documenti pubblicati. Ogni volta che un documento pubblicato soddisfa tali criteri, una notifica viene inviata al destinatario sottoscritto. Grazie a questo modulo, possono essere attivate le integrazioni con conservazione sostitutiva e FSE-INI, nonché resa disponibile l'infrastruttura di interfacciamento con gli MMG.

Gestione Consenso e Privacy

Nell'ambito del processo di gestione della privacy del cittadino, il sistema è pienamente integrato con il modulo funzionale di gestione consensi per risolvere le problematiche legate alla raccolta e gestione dei documenti di consenso del Cittadino, secondo le norme in vigore (D.Lgs. 193/2003) garantendo l'accesso ai dati clinici del singolo paziente esclusivamente agli operatori aventi tale autorizzazione.

Questo modulo affianca e completa le funzionalità generali di autenticazione, autorizzazione e *single sign-on* con la gestione della raccolta e indicizzazione dei consensi e preferenze di privacy espressi dal paziente, siano essi riferiti ai propri dati anagrafici o a determinati episodi di cura, così come mediante regole di accesso basate sui consensi stessi, che permettono di filtrare le richieste di fruizione dei dati protetti.

Gestione dell'integrazione anagrafica pazienti e medici

Modulo chiave dell'architettura, fornisce la possibilità di far cooperare i sistemi con una gestione centralizzata delle informazioni sul paziente all'interno dell'organizzazione, garantendo l'identificazione univoca del soggetto di cura, un pilastro imprescindibile per ottenere elevati livelli di qualità del dato, raggiungendo così l'obiettivo di offrire un sistema fortemente orientato all'accessibilità ed all'interoperabilità, alla tracciabilità delle operazioni ed all'unicità dell'informazione.

Gestione Terminologie

Grazie a questo modulo l'uso di codifiche omogenee, complete e corrette a livello clinico-sanitario diviene possibile, sia all'interno del sistema sanitario che negli scenari di integrazione ed interoperabilità. In quest'ultimo caso, infatti, l'aderenza agli standard va integrata con una gestione efficiente delle terminologie per poter garantire interoperabilità semantica. Le componenti funzionali messe a disposizione da questo modulo consentono di gestire con grande flessibilità il ciclo di vita di risorse terminologiche e di sistemi di mappatura/alias, che impiegati dagli altri moduli consentono di raggiungere i risultati attesi dalla S.A.

Audit Transazioni

Grazie alle funzionalità che espone, gli altri moduli possono attivamente tracciare tutte le attività di interesse all’interno del processo di lavoro che li coinvolge, mettendo a disposizione degli utenti amministratori un potente strumento di indagine e verifica dei principali eventi che hanno coinvolto il sistema. Abbiamo scelto di affidarci al modello funzionale proposto da IHE con il profilo ATNA.

Orchestrazione, definizione e monitoraggio dei processi

Costituisce l’insieme di strumenti necessari a consolidare e condividere percorsi di cura ed amministrativi, mettendo al centro del processo la persona. Questi strumenti sono resi disponibili a tutto il resto della soluzione: sfruttandoli, è possibile far cooperare i diversi attori coinvolti in un processo affinché questo possa essere gestito in modo efficiente dal suo inizio e lungo tutto il suo arco temporale, grazie all’uso di un insieme di regole, azioni e stati che lo compongono.

Integrazione, interoperabilità e aderenza allo standard

Espone le funzionalità necessarie a gestire i flussi di messaggistica, le transazioni IHE, nonché altre tipologie di messaggi in ingresso o uscita dai moduli funzionali che lo sfruttano. Lo fa attraverso l’impiego di una serie di connettori, ciascuno dei quali rappresenta un set di funzionalità ben definito. Si occupa inoltre di monitorare i flussi gestiti attraverso questi connettori, garantendo così una tracciatura delle attività intercorse.

3.3.2. SPECIFICHE TECNICHE

Di seguito sono descritte le funzionalità ed i servizi resi disponibili dalla piattaforma di Population Health Management (PHM) attraverso le proprie componenti “core”.

La piattaforma è stata progettata e realizzata in conformità ai profili di integrazione promossi da IHE che permettono di superare il concetto di collegamento punto – punto, implementando un vero e proprio motore di PHM capace di generare valore per i pazienti e per il sistema sanitario. A tale riguardo la piattaforma introduce un metodo ed una tecnologia per la condivisione dei dati, la gestione dei processi clinici, sanitari ed amministrativi, il coinvolgimento di attori sia ospedalieri sia operanti sul territorio come i Medici di Medicina Generale (MMG) ed i Pediatri di Libera Scelta (PLS), il paziente stesso, le strutture per la gestione delle cure primarie, le farmacie territoriali, ecc.

La piattaforma, in particolare, abilita una reale condivisione di dati, informazioni e documenti tra sistemi (anche esterni all’Ente) consentendo agli operatori clinici di accedere ai dati dei pazienti, anche storici e prodotti da differenti sistemi, e offrendo a tutti gli attori operanti nella Sanità,

nonché allo stesso Cittadino, di attivare forme più o meno evolute di accesso alle informazioni cliniche e alla documentazione prodotta dalle diverse strutture sanitarie coinvolte.

Il set dei servizi di interoperabilità gestiti dalla Piattaforma è piuttosto ampio, di seguito quelli che fanno parte del progetto.

Single-Sign-On (SSO), Security Token Service (STS) e Anagrafe degli Operatori

Il Security Token Service (STS) è uno standard aperto multipiattaforma dei servizi Web WS-Trust OASIS. Questo modulo prevede il rilascio di un token di identità basato su “claim” (attributi dell’utente), il servizio è responsabile per l'emissione, la convalida, il rinnovo e l'annullamento dei token di sicurezza. I token rilasciati dall’STS saranno utilizzati da un client che richiede l'accesso ai servizi esposti dalla piattaforma. In questo scenario non sono i servizi ad effettuare l’autenticazione verificando le credenziali di accesso ma è il modulo STS a rilasciante il token che sarà utilizzato per l’invocazione dei servizi da parte del cliente.

Il Token rilasciato dall’STS di piattaforma è di tipo SAML2 (Security Assertion Markup Language), si tratta quindi di un XML contenente attributi relativi all’identità di un operatore oltre a informazioni di sicurezza relative alla durata e all'emittente. Il token è protetto dalla manipolazione con crittografia avanzata. Il client presenta quindi il token a un'applicazione per accedere alle risorse fornite dall'applicazione.

Enterprise Service Bus (ESB) integrato e Message Asset Management (MAM)

Elemento cardine della piattaforma è l’Enterprise Service Bus (ESB) realizzato come un framework software specificatamente progettato per gestire l’intero ciclo di vita del software di integrazione nelle Strutture della Sanità, dalla sua specifica, progettazione e realizzazione alla sua esecuzione e gestione operativa.

La componente ESB oltre a coprire la totalità delle esigenze di interoperabilità di una singola Azienda è progettato per fornire supporto alla gestione della interoperabilità nell’ambito di una Federazione di Aziende quando lo scopo dell’integrazione, come nel caso di un Fascicolo Sanitario Elettronico, coinvolge più strutture sanitarie distribuite facenti parte di Enti sovra Aziendali, come Aree Vaste e Regioni.

Tutte le componenti dell’ESB sono state progettate e realizzate conformemente agli standard di integrazione adottati nella sanità (HL7, IHE, DICOM…) e con l’obiettivo di soddisfare le due principali esigenze dell’Utenza:

1. acquisire in tempi brevi software di integrazione con un elevato livello di qualità, facilmente mantenibile ed a costo contenuto;
2. disporre di strumenti facili da usare e dotati di tutte le funzioni necessarie per monitorare e controllare la gestione operativa del software di integrazione ed il patrimonio di messaggi gestiti con l’ESB.

Nel seguito di questo documento, dopo un’analisi della struttura dell’offerta di Piattaforme di integrazione, saranno descritti i punti di forza che caratterizzano ESB, ovvero:

1 Ambiente di sviluppo che copre l’intero ciclo di vita del software di integrazione con generazione automatica dei Canali di integrazione e dei Router a partire dalle Specifiche;
2 Riuso integrale di Canali di integrazione a Catalogo;
3 Strumenti avanzati di Gestione del patrimonio di messaggi (MAM).

Scalabilità delle performances

La scalabilità delle performances del modulo ESB dipende dalle risorse HW disponibili, dal numero di Pipeline paralleli utilizzati nell’integrazione e dall’uso eventuale di una configurazione a cluster.

A titolo di esempio su un PC con processore Intel i7 a 2.5 Hhz e 4 GB di RAM per trasportare 1.000 messaggi, relativi ad un solo pipeline di integrazione (una sola applicazione mittente invia in successione i messaggi su un solo entry point di ESB, attendendo, prima di inviare il messaggio successivo che ESB gli restituisca l’ACK ricevuto dall’applicazione destinataria), impiega circa 20 secondi, ovvero è in grado di trattare circa 50 messaggi sincroni al secondo.

Nel caso che una istanza di ESB sia configurata per gestire più pipeline di integrazione, come solitamente avviene in casi reali per la gestione parallela di più Message Type, una istanza di ESB è in grado di veicolare diverse decine di migliaia di messaggi al minuto. Nello specifico, utilizzando un PC con le caratteristiche sopra descritte, i messaggi trasmessi da una istanza di ESB su 20 pipeline di integrazione paralleli sono circa 850 al secondo.

Un cluster di 3 istanze di ESB, configurato ciascuno su 20 pipe di integrazione paralleli, è in grado di supportare picchi di lavoro superiori alle 2.500 transazioni al secondo.

Strumenti di Message Asset Management (MAM)

I vantaggi per l’Utente finale del sistema integrato sono dovuti alla economicità e qualità del software di integrazione, illustrate nel capitolo precedente, ed alla disponibilità di strumenti di Message Asset Management (MAM) per il monitoraggio e controllo delle attività (BAM) e dei livelli di servizio (SLM) della messaggistica, estremamente evoluti e sofisticati, oggetto di questo capitolo.

Questo è stato reso possibile dalla decisione di implementare le integrazioni non tramite l’uso di servizi per l’accodamento della messaggistica general purpose quali JMS (che forniscono strumenti predefiniti di monitoraggio e controllo sulle code e quindi non facilmente personalizzabili ed estendibili) bensì direttamente su una Base Dati progettata per ottimizzare l’efficienza nella gestione delle strutture dati di supporto agli strumenti per il monitoraggio e controllo della messaggistica.

La disponibilità di un Data Base progettato ad hoc, su cui è consentito un accesso diretto e senza vincoli, ha consentito di sviluppare intorno alla componente ESB una vasta gamma, oggetto di continua evoluzione, di servizi e di strumenti di Business Activity e Service Level Monitoring tra cui una Consolle per il Monitoraggio e la gestione via Web dell'Asset di messaggi in transito, un sistema di gestione di Report statistici ed un Repository a lungo termine per la conservazione dei messaggi transitati su ESB.

Consolle di Monitoraggio Aziendale

È accessibile localmente all'Azienda come Applicazione web tramite un internet browser, e da remoto previa creazione di una VPN con il server che ospita una installazione di ESB. Dalla Console sia il Progettista delle integrazioni che l'Utente finale possono analizzare in dettaglio il comportamento del sistema, delle applicazioni integrate, delle interazioni implementate ed il corrispondente flusso dei messaggi. In caso di malfunzionamenti è possibile intervenire per ripristinare il sistema. L'interfaccia utente implementata dalla Consolle, vedi figure seguenti, espone all'operatore una vista sul software di integrazione che rispetta la metafora del Pattern di integrazione presentando, al più alto livello di astrazione, le applicazioni integrate, i loro canali di integrazione, il router ed eventualmente i gateway realizzati per implementare lo scenario di integrazione.

MPI (Master Patient Index)

L'anagrafe centralizzata rappresenta un modulo cardine nell'architettura di un sistema informativo sanitario, in quanto punto di riferimento unico per la gestione delle informazioni relative al paziente, sia quelle di carattere prettamente anagrafico (nome, cognome, data di nascita, residenza, …) che quelle di natura sanitaria (ad esempio, nella realtà italiana, le informazioni sull'ASL di assistenza ed esenzioni, oppure per l'estero informazioni relative alle assicurazioni sottoscritte).

Al fine di proporre una gestione flessibile e configurabile delle informazioni, MPI gestisce un set di dati predefinito e offre la possibilità di aggiungere un set di dati personalizzato per installazione.

MPI offre web services di interoperabilità anagrafica che implementano gli standard internazionali HL7/IHE per gestire la ricerca, l'inserimento/aggiornamento e il merge di record anagrafici.

I dipartimentali che dispongono di una propria anagrafe locale possono gestire la sincronizzazione tramite opportuna sottoscrizione ai servizi di notifica delle variazioni (profilo PIX), per ricevere in tempo reale gli aggiornamenti della base anagrafica centrale.

MPI, tramite un'interfaccia web, offre diverse funzionalità di backoffice, quali ad esempio:

- sottoscrizione ai servizi di notifica e configurazione degli attori
- ricerca e aggiornamento manuale dei record anagrafici
- visualizzazione dello storico delle variazioni anagrafiche
- merge tra due posizioni anagrafiche

DiTAM

L’obiettivo di questa componente è di poter disporre di un unico strumento di gestione centralizzata delle codifiche aziendali (es. Catalogo Prestazioni, Codici ICD-9, Reparti, ecc.) e di un sistema di notifica delle variazioni operate alle anagrafiche centrali e condivise.

DiTAM (Distributed Terminology Assets Management – gestore distribuito di risorse terminologiche in Italiano) è una infrastruttura software distribuita, basata su standard, aperta ed estensibile che supporta la produzione, manutenzione ed utilizzo di risorse terminologiche.

DiTAM è una soluzione flessibile, scalabile e aderente a standard internazionali al problema di creare, manutenere, distribuire e rendere operative le risorse terminologiche di un'organizzazione – siano queste semplici tavole di codifica o rappresentazioni complesse di termini e conoscenza, quali tassonomie di termini, o vere e proprie ontologie con classificazioni multiple di concetti. DiTAM fornisce interfacce e servizi a supporto di “sistemi” e di singoli individui, siano questi persone, organizzazioni o sistemi informatici, in un contesto locale o geograficamente distribuito.

In termini di flusso, ciascun sistema verticale allinea, al momento della configurazione, le proprie codifiche con quelle costituenti la codifica regionale usufruendo dell’interfaccia utente esposta dal modulo DiTAM.

Attraverso le funzioni di back-office di DiTAM è possibile verificare la completa copertura della mappatura delle codifiche.

In estrema sintesi, il servizio centrale DiTAM supporta:

- la fase di mappatura tra le codifiche dei sistemi verticali e quelle regionali (anagrafi strutture sanitarie, Personale sanitario, codifica regionale per l’anatomia patologica, …), fornendo un riscontro, in tempo reale, della correttezza dei dati inseriti;

- ogni comunicazione tra sistema verticale e piattaform, preoccupandosi della transcodifica dei codici e, quindi, consentendo al sistema verticale di conservare la propria codifica interna nelle comunicazioni.

Quest’ultimo aspetto rappresenta una significativa facilitazione nel processo di integrazione di eventuali nuovi sistemi, in quanto supera la problematica dell’implementazione presso i sistemi verticali di moduli applicativi di decodifica basati su di una duplicazione delle tabelle di decodifica dei codici prestazione utilizzati localmente.

La gestione delle terminologie non coinvolge solo problematiche di natura tecnica. La gestione di risorse distribuite e complesse richiede strumenti per definire, specializzare e attuare Politiche di gestione delle risorse che coinvolgono insieme Strutture organizzative, Utenti umani ed applicativi e Risorse terminologiche. A questo scopo DiTAM:

- Consente di modellare, tramite la GUI Web, l’organizzazione della produzione delle risorse terminologiche tramite la definizione di Unità Organizzative tra cui ripartire le attività di gestione all’interno del DITAM.

- Consente di configurare Politiche di accesso, tramite la GUI Web, per abilitare specifici utenti ad operare, con un ruolo specifico, su specifiche Risorse terminologiche o Unità organizzative con le modalità permesse dal ruolo a loro assegnato.
- Consente di associare ad ogni Ruolo un insieme definito di Autorizzazioni predefinito per default in fase di installazione ed avviamento ma riconfigurabile via GUI a regime nel corso dei lavori.
- Consente la definizione e gestione di nuovi Ruoli associati ad insiemi definiti di Autorizzazioni
- Controlla che solo gli Utenti umani ed applicativi associati ad una Unità organizzativa abbiano accesso alle Risorse terminologiche associate alla Unità.
- Consente di configurare, nell'ambito del DITAM, Gerarchie di Unità organizzative tali che gli Utenti associati ad una Unità abbiano visibilità su tutte le Risorse terminologiche associate alle Strutture organizzative di livello superiore nella gerarchia. Questo per consentire a più Unità organizzative di livello inferiore (dedicate ad esempio alla gestione di terminologie derivate: Value Set Definition o Map Version) di condividere l'accesso a risorse terminologiche comuni (Es. Code System Version di Nomenclatori standard internazionali, nazionali o regionali)

L'efficienza, l'affidabilità e la usabilità dei sistemi di gestione di risorse terminologiche sono esaltate se si forniscono ad utenti umani ed applicativi modalità di interazione avanzate e non solo limitate alla GUI o alle API standard. A questo scopo DiTAM:

- fornisce (ad Utenti umani ed applicativi) Servizi di Sottoscrizione di risorse terminologiche e di revisione di risorse terminologiche
- fornisce (ad Utenti umani ed applicativi) Servizi di Notifica di disponibilità o revisione di risorse terminologiche
- fornisce (ad Utenti applicativi) Servizi di Delivery automatico di risorse terminologiche con protocolli e formati standard (XML, CSV, HL7 MasterFile…) al fine di consegnare alle applicazioni risorse terminologiche aggiornate rispetto alla evoluzione e gli aggiornamenti apportati in Back Office alle risorse terminologiche in DITAM.

Registry e Repository Documentali

La gestione dei documenti sanitari si basa su componenti software cooperanti, tra le quali assumono particolare rilievo i moduli applicativi XDS.b Registry e XDS.b Repository. Queste due componenti, costituenti il modulo XDS, cuore della Piattaforma, implementano le funzionalità previste dagli omonimi attori protagonisti del profilo d'integrazione IHE-XDS.b, su cui si fonda il paradigma di condivisione/gestione documentale implementato dall'engine della piattaforma. Questo profilo di integrazione consente, tra l'altro, la gestione di documenti strutturati secondo lo standard CDA2 di HL7, nonché l'adozione degli standard ebXML 3.0, SOAP v1.2 ed MTOM/XOP.

Il componente Repository è incaricato della gestione della persistenza dei documenti informatici ed è normalmente distribuito a livello aziendale (ASL/AO). Il profilo XDS.b prevede la presenza di

uno o più Repository. Ogni Repository offre le funzionalità base di archiviazione e recupero di un determinato documento a partire da un suo riferimento.

Il componente Registry rappresenta l’indice documentale. Contiene l’insieme dei metadati relativi ai documenti archiviati sui Repository e permette di effettuare le ricerche su questi ultimi, conformemente ai diritti di accesso dell’utente richiedente. Il profilo di integrazione IHE XDS.b prevede la presenza di un solo Registry. La ricerca può quindi avvenire verso il Registry unico che indicizza tutti i documenti ed i risultati di una certa ricerca indirizzano sul particolare Repository da cui recuperare il documento.

Gestore delle Notifiche (DSUB)

Il sistema di notifica presente nella piattaforma rappresenta il componente attraverso il quale la piattaforma svolge un ruolo attivo. Esso si basa sul profilo d’interazione IHE DSUB.

Il sistema di notifica consente di informare un’applicazione di un evento accaduto nell’ambito della Piattaforma come, ad esempio, la pubblicazione di un documento nel Repository per il quale l’applicazione ha manifestato interesse attraverso la sottoscrizione. In particolare, la Piattaforma è già pronta per instradare notifiche relative alla disponibilità di referti ai Medici di Medicina Generale / Pediatri di Libera Scelta le cui cartelle cliniche sono riconosciute dalla Piattaforma e i cui pazienti abbiano acconsentito l’accesso ai referti.

Viewer Documentale

La piattaforma di interoperabilità mette a disposizione un modulo Viewer documentale, a corredo dell’infrastruttura XDS.b del pacchetto Repository/Registry, che fornisce un’interfaccia di accesso ai documenti clinici del paziente.

Le caratteristiche del Viewer consentono l’utilizzo secondo le seguenti modalità operative:

- come applicativo web “standalone” per l’accesso fuori contesto da parte degli operatori sanitari. Gli utenti che si trovano fuori dal contesto ospedaliero, debitamente abilitati e profilati, possono accedere via web alla storia clinica di un paziente, per condividere documenti con i colleghi o per rispondere alla richiesta di consulto da parte del paziente stesso e da parte di altri medici. La sicurezza dei dati è garantita dalle regole di accesso fornite dall’infrastruttura e dall’uso del protocollo HTTPS;
- richiamato in “contesto”, come funzionalità di un applicativo. Questa modalità consente di richiamare le singole funzionalità di consultazione e/o rendering senza uscire dal contesto funzionale, ma semplicemente navigando tra le informazioni del paziente (esempio: è possibile utilizzare il Viewer per il solo rendering di un singolo documento).

Il tipico flusso operativo prevede un’apertura in contesto, che consente ad applicazioni di terze parti di invocare specifiche funzionalità (azioni) messe a disposizione dal Viewer, separando il Viewer stesso dal loro workflow applicativo.

L'utente può selezionare il paziente direttamente dal proprio applicativo di riferimento (ad esempio da una "Lista Pazienti") e a questo punto l'applicativo potrà passare l'identificativo del paziente al Viewer che provvederà a cercare sulla Piattaforma tutti i relativi documenti (eventualmente considerando un filtro di ricerca, passato anche quello), e a presentarne la lista.

La successiva azione possibile può essere quella di cercare, estrarre e visualizzare un certo documento richiesto dall'utente. Alla fine delle operazioni il controllo può tornare all'applicativo chiamante.

Questo approccio è reso possibile:

- dalla natura completamente web della soluzione, caratterizzata da un'interfaccia utente coesa ed omogenea;
- dal sistema di Single Sign-On;
- dal sistema di condivisione del contesto.

Consent Manager

Come risultato della progressiva digitalizzazione dell'informazione e della società, anche i rapporti tra il cittadino e lo stato, nonché le modalità di fruizione dei servizi, stanno mutando. Sempre più aspetti della quotidianità vengono mediati da sistemi informatici sempre più connessi tra loro. La mole dei dati all'interno di tali sistemi è in crescita continua, e così la loro gestione ed utilizzo sono materia di ricerca, al fine di migliorare la comprensione che ciascun organismo o servizio ha dei propri fruitori, facilitare l'accesso e aumentare l'efficienza.

La sanità è certamente uno dei settori che più possono trarre beneficio dall'informatizzazione di dati e procedure. Tuttavia, assieme alle opportunità che ciò offre alla popolazione nel suo complesso, si riscontra anche la necessità di tutela dei singoli cittadini. I dati personali, definiti come ogni informazione individuata o individuabile relativa ad una persona fisica, in particolare sono merce preziosa.

Nell'ambito della protezione dei dati personali entrano in gioco i concetti fondamentali di sicurezza e privacy. La sicurezza è l'insieme delle misure che il titolare della gestione dei dati deve rispettare per proteggerli, qualunque essi siano, anche se si tratta di dati non strettamente personali e a prescindere dal fatto che si tratti di dati sensibili o meno, ovvero rappresenta un quadro normativo generale.

Dall'altro lato le norme sulla privacy regolano specificamente la manipolazione ed il trattamento dei dati personali, in ultima analisi con l'intento di restituire al cittadino il controllo sui propri dati. In virtù di questa distinzione, spesso si dice che può esserci sicurezza senza privacy, ma non può esserci privacy senza sicurezza.

Dal punto di vista normativo, il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation – Regolamento UE 2016/679), destinato ad entrare in vigore nel 2018, rafforza e unifica la protezione dei dati personali a livello europeo.

Il regolamento introduce nuove disposizioni in materia di privacy, tra le quali l’obbligo per autorità pubbliche titolari dell’elaborazione dei dati di nominare un funzionario per la protezione dei dati (Data Protection Officer, DPO), configurando uno scenario in cui è fortemente accentuata la responsabilità della singola struttura.

Nell’ottica di permettere al cittadino di esercitare il proprio diritto alla privacy e determinare le regole di visibilità dei propri dati sanitari, la Piattaforma di interoperabilità integra una componente per la gestione di regole, denominata Policy Manager.

Caratteristiche Funzionali

Il modello di gestione del consenso centralizzato, i relativi servizi esposti e le componenti funzionali offerte dal modulo Consent Manager supportano da un lato i moduli di piattaforma che, per le funzioni implementate, hanno necessità di effettuare verifiche sui consensi del cittadino, dall’altro i client che intendano integrare nei propri flussi la gestione dei consensi. Le componenti funzionali offerte, descritte più in dettaglio nei paragrafi successivi, sono le seguenti:

- acquisizione e modifica Consensi: un insieme di servizi trasversali utilizzabili per leggere, inserire, revocare e modificare i consensi attraverso APIs REST e tramite una interfaccia GUI che permette all’operatore di raccogliere le informazioni di consenso attraverso apposite maschere configurabili;
- visualizzazione Consensi Paziente, Episodio, Documento: un insieme di servizi REST ed un set di componenti fruibili con interfaccia utente (widget) richiamabili in contesto da applicazioni esterne;
- un insieme di funzionalità centralizzate di amministrazione ed applicazione delle policy (Policy Manager), per consentire sia la configurazione delle politiche di accesso alle risorse (documenti e informazioni strutturate) di piattaforma, sia il controllo degli accessi a tali risorse.

Tipologie di consenso gestite

La soluzione può abilitare la gestione di tre diversi livelli di consenso, che determinano altrettanti perimetri di validità delle preferenze in materia di privacy espresse dall’assistito.

Paziente: concede o nega un consenso generale la cui validità si estende a tutti i documenti ed informazioni strutturate riferiti all’assistito stesso. Questo è il consenso di più alto livello e può essere ad esempio usato per oscurare un interno dossier clinico e inibire qualsiasi modifica o aggiunta futura senza dover esplicitare altre preferenze.

Evento: concede o nega un consenso la cui validità si estende a tutti i documenti ed informazioni strutturate prodotti nell’ambito di un medesimo evento clinico, ad esempio un ricovero (fino alle dimissioni), oppure una visita ambulatoriale. Rappresenta un livello intermedio di consenso.

Documento: concede o nega un consenso riferito ad un singolo documento clinico, inclusi eventuali suoi allegati, senza fornire indicazioni su altri documenti anche connessi ad un medesimo evento clinico. Questo è il consenso di più basso livello e garantisce all’assistito il massimo controllo sulla visibilità dei propri dati sensibili.

Audit

Sempre più frequentemente le aziende sanitare coinvolte nel processo di cura scambiano informazioni private o sensibili relative ai pazienti, sia all’interno dei loro sistemi informativi che da e per altri sistemi.

Questo scambio di informazioni deve essere costruito su una piattaforma che dia al sistema garanzia di aderenza ad un modello robusto di security e privacy, governando un accesso ai documenti e dati sensibili sicuro, ristretto, tracciato e riconducibile ad un’identità precisa.

Tale modello si basa sulla messa in opera di una serie di policy organizzative, funzionali e tecniche aventi come oggetto l’interoperabilità e lo scambio di informazioni; policy che sono realizzabili grazie all’impiego di alcuni moduli funzionali indispensabili in scenari di cooperazione applicativa.

Tra questi è fondamentale la presenza di un modulo che consenta l’ ”auditing” ed il “reporting” di eventi rilevanti da un punto di vista di privacy e sicurezza all’interno del sistema, permettendo ai sistemi interessati di registrare gli eventi significativi, ed agli addetti incaricati del controllo della sicurezza di verificare l’aderenza dei sistemi e degli operatori che li utilizzano alle policy definite all’interno dell’organizzazione.

Caratteristiche Funzionali

La piattaform, per realizzare le funzionalità sopra descritte, rende disponibile il modulo di “Audit Record Repository”. Il modulo aderisce al profilo standard internazionale IHE ATNA: tale profilo consente di implementare il modello aziendale di security e privacy sfruttando transazioni e standard di comunicazione omogenei.

In particolare, la componente Audit Record Repository della piattaforma supporta i flussi di:

- pubblicazione di nuovi Audit Event
- ricerca, filtraggio e recupero di Audit

Accesso agli Audit Event

“Audit Record Repository” mette a disposizione diversi strumenti per il recupero, da parte di un Audit Consumer, delle informazioni relative ad eventi di audit all’interno dell’Audit Record Repository. Gli audit record contenuti nel repository vengono automaticamente indicizzati e trasformati in risorse FHIR: diventano dunque disponibili per l’interrogazione in base ad una serie di criteri di ricerca.

Il recupero di eventi di Audit (AuditEvent) opportunamente filtrati può rappresentare un valido strumento per diversi scenari, quali ad esempio:

- raccolta di una cronologia di interventi clinici effettuati con differenti device, per consolidare una fotografia completa del caso clinico

- valutazioni sugli effettivi accessi alla storia documentale di un paziente a fronte dei consensi espressi dal cittadino
- monitoraggio statistico dell’utilizzo dei flussi documentali (anche per eventuali valutazioni di carico)

3.3.3. SPECIFICHE DI COMUNICAZIONE

L’architettura a servizi (SOA) e a risorse (ROA) definita per la piattaforma, consente un utilizzo parziale dell’intero set di funzionalità offerte dalla piattaforma stessa. Di seguito un dettaglio delle componenti funzionali previste dal progetto e come queste insistono sui moduli della piattaforma.

Funzionalità “Aggregatore”	Modulo piattaforma
STS - RequestSecurityToken	Modulo autenticazione STS
XDS - Web Service - ITI-41 ProvideAndRegisterDocumentSet	Modulo XDS.b Repository
Lettura dati TS/CNS	Modulo Invio Documenti ad FSE[INI]/Browser
Integrazione INI - Client - ComunicaMetadati	Modulo Invio Documenti ad FSE[INI]
ListaRefertiPertinenzaUtente	Modulo Invio Documenti ad FSE[INI]
CercaRefertiPertinenzaUtente	Modulo Invio Documenti ad FSE[INI]
VisualizzaDocumento	Modulo Invio Documenti ad FSE[INI]

Modulo autenticazione STS

Si tratta di un servizio Web Services standard WS-Trust per l’acquisizione di un token di autenticazione.

Di seguito le specifiche:

Operation: “RST/Issue”

Action Header: http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue

WSDL : http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.html#_Toc325659000

Body Element: Secondo la specifica WS-Trust, la richiesta di un token di sicurezza assume la forma dell'elemento “RequestSecurityToken” secondo il seguente namespace “http://schemas.xmlsoap.org/ws/2005/02/trust”, definito dallo schema:


sts.xsd

ProvideAndRegisterDocumentSet

La transazione utilizzata è quella prevista dalle specifiche del profilo IHE XDS.b nello specifico la transazione ITI-41 “ProvideAndRegisterDocumentSet-b”. Di seguito le specifiche del servizio e gli oggetti che rappresentano un esempio di messaggi scambiati:


response_ITI-41.txt


request_ITI-41.txt

XML schema definition XSD

I seguenti oggetti rappresentano lo schema XSD di riferimento


XDS.b_DocumentRepository.xsd

XML schema definition WSDL

I seguenti oggetti rappresentano i WSDL di riferimento dei servizi


XDS.b_DocumentRepository.wsdl

Lettura dati TS/CNS

L’autenticazione ai servizi viene effettuata secondo le specifiche definite da INI nel “Kit Tecnico di FSE[INI]”. Tutti i servizi sono esposti su canale “https” con protocollo di sicurezza TLS 1.2.

Integrazione INI - Client – ComunicaMetadati

L’integrazione è quella definita nelle specifiche INI nel “Kit Tecnico di FSE[INI]”.

XML schema definition XSD

I seguenti oggetti rappresentano lo schema XSD di riferimento


ComunicazioneMetadatiRichiesta.xsd


ComunicazioneMetadatiRicevuta.xsd

WSDL


fseComunicazioneMetadati.wsdl

3.4. MODULO INTERFACCE STAKEHOLDERS

Attraverso la realizzazione di un Servizio Private Cloud centralizzato di aggregazione (di seguito “Aggregatore”), vengono rese disponibili un insieme di funzionalità dette “acceleratori”, che consentono di semplificare e velocizzare i processi di integrazione al FSE[INI], altrimenti demandati ai singoli sistemi stakeholders che hanno un alto livello di frammentazione (fisica ed applicativa) sul territorio.
La soluzione, gestita centralmente, fornisce una partizione dedicata ad ogni stakeholder, come estensione del sistema, in modo che quest’ultimo si presenti con le proprie credenziali ed il proprio indirizzo IP alle interfacce applicative di FSE[INI] sfruttando le più efficaci e innovative tecnologie di Cloud Computing e nel pieno rispetto delle norme e delle linee guida in materia di FSE.
Nella partizione dedicata ciascuno stakeholder ha a disposizione funzioni e servizi che altrimenti sarebbero soggetti a molteplici installazioni e verifiche individuali, ottimizzazione della verifica di correttezza ed integrità del messaggio nel suo formato di invio e di pubblicazione dei documenti sul FSE[INI]. Le verifiche effettuate dall’Aggregatore non entrano nel merito del contenuto e non effettuano trasformazioni o duplicazioni dei documenti.

Dal punto di vista tecnico i moduli funzionali principali dei servizi in Cloud di aggregazione e della partizione virtuale per Laboratorio sono:

- Modulo per la Firma Digitale Remota
- Modulo per la generazione dei CDA2 semplificata
- Modulo SDK per la comunicazione
- Modulo di cache documenti

- Client per l’autenticazione ai servizi TS/CNS
- Modulo di trasmissione dei documenti ad FSE[INI]

Per tutelare l’operatività in regime di riservatezza nonché un accesso esclusivo ai dati che transitano sull’aggregatore, mantenendo al contempo i vantaggi funzionali dati dalla centralizzazione delle funzionalità “acceleratori”, il modello di distribuzione prescelto è quello della “singola istanza con partizionamento logico”. Il servizio di Firma Digitale Remota è affiancato ad ogni partizione logica assegnata al singolo stakeholder. I moduli funzionali ospitati dall’aggregatore sono infatti esposti secondo una logica di partizionamento esclusivo: in particolare, a ciascun stakeholder è assegnata una partizione di lavoro dedicata ed esclusiva. Questa partizione contiene sia gli acceleratori funzionali che i dati e costituisce un perimetro sicuro di accesso da parte della singola utenza. Le funzionalità sono appositamente progettate per lavorare secondo partizioni, non è dunque possibile per un utente assegnato ad una partizione accedere a funzionalità o dati contenuti in un’altra.
Il modello scelto è simile a quanto già esistente nel mondo hardware e di sistemi operativi mediante l’uso dei thread: ciascun processore è in grado di far girare contemporaneamente più di un processo “logico” (macchina vituale), ma i dati e il contesto di esecuzione di ciascun processo logico sono inaccessibili agli altri, pur essendo uno solo il processore che li esegue.
Nei paragrafi seguenti ciascuno dei moduli funzionali introdotti viene descritto in dettaglio, specificando le sue componenti funzionali e l’uso previsto. Viene inoltre data una visione delle caratteristiche di sicurezza e della gestione della privacy dei dati.

3.4.1. MODULO DI FIRMA DIGITALE REMOTA

Questo modulo è parte integrante dei servizi messi a disposizione dal Cloud Regionale dei Servizi di Aggregazione al fine di fornire agli operatori stakeholder un set completo di servizi in Cloud, utilizzando metodi, procedure e tecnologie fornite dalla Certification Authority individuata dalla Regione, che per la loro natura si affiancheranno ai servizi descritti nei paragrafi successivi con la stessa modalità e filosofia di fornire un’ambiente semplificato, partizionato e dedicato ad ogni singolo stakeholder.

3.4.2. MODULI SDK

I due moduli SDK sono al servizio dei sistemi stakeholder al fine di semplificare al massimo il loro processo di integrazione con l’Aggregatore. La finalità con cui sono distribuiti è quella di togliere ai servizi di refertazione ogni complessità legata alla comunicazione a messaggi e alla produzione di documenti complessi, consentendo loro di lavorare mediante semplicissime chiamate ad oggetti implementate nel linguaggio loro più congegnale. Gli SDK sono forniti infatti sia in tecnologia Java che in tecnologia .NET. L’esperienza maturata dimostra che mediante questo approccio è possibile ridurre i tempi di implementazione delle integrazioni con i vari sistemi di oltre il 70%.

3.4.3. MODULO CLIENT PER AUTENTICAZIONE TS/CNS

Questo modulo funzionale mette a disposizione dei sistemi stakeholder servizi che consentono di uniformare e concentrare l’applicazione “client” di gestione dell’autenticazione TS/CNS, necessaria per inviare i documenti a FSE[INI], nel pieno rispetto della normativa e della identificazione dell’operatore.
Il modulo si pone come servizio a supporto dei sistemi stakeholder, senza costituire un sistema intermedio: esso infatti espone al sistema stakeholder il client per la gestione del processo di autenticazione consentendo esclusivamente al sistema stakeholder di eseguirla all’interno del proprio ambiente applicativo.
Si tratta dunque di una funzionalità esposta lato Aggregatore per poter essere eseguita lato stakeholder. In questo modo, il canale di comunicazione sicuro che viene stabilito, pur essendo facilitato da questo modulo funzionale, è una connessione diretta tra la macchina che fa girare il sistema stakeholder, sulla quale è fisicamente presente il lettore di smart card TS/CNS, e i server di FSE[INI] che espongono i servizi protetti da tale tipologia di autenticazione.
Il beneficio principale dato dalla disponibilità di questo modulo funzionale è la possibilità di aggregare in un punto unico l’istanza di applicazione client per il processo di autenticazione e di raccordarlo con grande facilità con quello di invio dei documenti a FSE[INI], a tutto vantaggio dei tempi di esecuzione del progetto, dei costi operativi e della semplificazione del processo di assistenza e manutenzione. L’operatore della struttura sanitaria che invia al sistema FSE[INI] è quindi il sistema stakeholder locale che autenticandosi con la TS/CNS stabilisce il canale sicuro e “diretto” tra il sistema stakeholder e il sistema FSE[INI].

3.4.4. MODULO DI GESTIONE CACHE DOCUMENTI

Questo modulo consente ai sistemi stakeholder di ottimizzare la fase di invio dei documenti a FSE[INI]. Si tratta di un modulo che mette a disposizione un’area di memoria “temporanea” di dimensioni contenute (meglio definibile come cache o caching) ma altamente efficiente, alimentando la quale è possibile rendere pressoché istantaneo agli operatori stakeholder il processo di invio dei documenti, riducendo i tempi di caricamento.
Grazie a questo modulo, inoltre, è possibile superare le possibili difficoltà tecniche legate a interruzioni o rallentamenti delle comunicazioni di rete da parte di alcuni sistemi stakeholder dislocati in nodi della rete regionale più critici (digital divide).
La memoria di cache consente di trasferire la gestione di questo tipo di problematiche dalla fase di invio ad FSE[INI], nella quale un operatore deve necessariamente presidiare il sistema, ad una fase preparatoria che il sistema stakeholder può gestire autonomamente. In questo modo, nel momento in cui l’operatore invia i documenti ad FSE[INI], ha la garanzia che qualora vi fossero problemi di connettività per il trasferimento dei documenti alla destinazione, tale contingency verrebbe superata attraverso l’Aggregatore Regionale.
Infine, tale modulo potrebbe abilitare anche una gestione dinamica di eventuali documenti per i quali l’invio a FSE[INI] fallisce per indisponibilità del sistema di destinazione. Senza l’impiego della cache tali invii andrebbero perduti, mentre il suo impiego garantisce che i documenti vengano mantenuti in cache per il tempo necessario a completarne l’invio ad FSE[INI] e gestiti automaticamente dall’Aggregatore, senza dover riversare su ciascuno dei sistemi stakeholder il compito di implementare le logiche di gestione richieste.

Il sistema di aggregazione controlla inoltre la correttezza dei documenti inviati, controllando che siano presenti:

- il referto strutturato in formato CDA2, con foglio di stile. In alternativa, fino a quando il sistema FSE[INI] ne consentirà il conferimento, il referto in formato pdf firmato in cades/pades
- I metadati obbligatori, quali:
    - Codice fiscale dell’autore
    - Ruolo dell’autore
    - Codice struttura di appartenenza
    - Codice fiscale del paziente
    - Tipologia del documento

Trattandosi di una memoria cache, il contenuto predisposto al suo interno gode delle proprietà tipiche di questo tipo di memorie:

- Ha una capienza limitata
- Ha prestazioni più efficienti rispetto all’invio non mediato da cache
- È protetta: crittografata ed accessibile unicamente ai sistemi stakeholder che la alimentano e utilizzano
- È partizionato secondo la gerarchia della cache
- È ad uso esclusivo dei sistemi stakeholder, non è accedibile da accesso umano, operatori o amministratori di sistema
- Contiene solo informazioni valide grazie ai meccanismi di validazione della struttura dei messaggi
- Tutti i suoi contenuti hanno una scadenza a breve termine: i documenti inviati ad FSE[INI] vengono immediatamente cancellati, mentre eventuali documenti non inviati sono rimossi dopo un limitato intervallo di tempo necessario a garantire la gestione del caso d’uso di mancato invio.

Il sistema consente di impostare, in fase di configurazione, il valore definito dai processi organizzativi e dalle procedure locali dei Laboratori per stabilire la durata temporale massima, di conservazione della cache dei documenti. Il valore di base è impostato a 6 giorni, passato tale range la cache dei documenti viene cancellata in modo permanente dal sistema. Si precisa che la cache dei documenti è un’area riservata ad accesso esclusivo dei sistemi stakeholder. Ogni stakeholder dispone di una propria area riservata e protetta di caching documenti. Quando i referti sono trasferiti nella cache vengono cancellati dal sistema stakeholder locale a garanzia della unicità dei documenti presenti nell’intero sistema per alimentare FSE[INI]

3.4.5. MODULO INVIO DOCUMENTI AD FSE

Questo modulo di comunicazione mette a disposizione dei sistemi stakeholder la funzionalità di invio dei documenti ad FSE[INI], realizzata mediante chiamata al servizio comunicaMetadati descritto nel Kit Tecnico di FSE[INI].
L’invio avviene in modo massivo e tecnologicamente uniforme per ogni singolo operatore, semplificando così il flusso di aggregazione dei soggetti del Servizio Sanitario Regionale ed FSE[INI],

realizzando di fatto il processo di centralizzazione di queste logiche in un unico servizio regionale pur mantendo l’identità ed il collegamento punto-punto fra i vari stakeholder ed FSE[INI].
Il modulo agisce in sinergia con altri due moduli funzionali della soluzione:

- Il modulo di gestione semplificata dell’autenticazione TS/CNS, che viene utilizzato dagli stakeholders per stabilire il canale sicuro impiegato per l’effettivo invio dei documenti
- Il modulo di gestione della cache documenti, impiegato per ottenere i documenti oggetto di invio a FSE[INI]

3.4.6. MODULO DI AUDIT E ANALISI

Grazie alle funzionalità che espone, gli altri moduli possono attivamente tracciare tutte le attività di interesse all’interno del processo di lavoro che li coinvolge mettendo a disposizione degli utenti amministratori un potente strumento di indagine e verifica dei principali eventi che hanno coinvolto il sistema (security by design).

3.4.7. CARATTERISTICHE DI SICUREZZA E PRIVACY DEI DATI GESTITI

Il sistema gestisce l’intero flusso di invio di documenti ad FSE[INI] in modo sicuro. Per farlo, il sistema assicura costantemente:

- L’autenticazione dell’origine di ciascuna richiesta a un servizio (Authentication)
- L’accesso selettivo ai servizi in base all’identificazione del chiamante (Authorization)
- Il mantenimento della privacy delle informazioni scambiate durante la comunicazione (Confidentiality)
- La garanzia dell’autenticità, integrità e non ripudiabilità delle informazioni scambiate (Integrity)

La strategia di sicurezza proposta copre tutti gli aspetti critici di un processo di messa in sicurezza di un sistema informativo:

1. Criptazione delle informazioni in transito (Encryption in transit)
2. Criptazione delle informazioni persistite (Encryption at rest)
3. Configurazione sicura dell’infrastruttura
4. Tracciatura ed analisi delle attività di accesso

L’autenticazione degli operatori, in linea con quanto previsto dal protocollo FSE[INI], è demandata direttamente ai sistemi stakeholder fruitori dei servizi, che si autenticano mediante TS/CNS.

Criptazione delle informazioni in transito

La soluzione tecnologia impiegata per la protezione dei canali di comunicazione prevede l’impiego dei protocolli di trasporto HTTPS / TLS.

TLS è lo standard de-facto nel mondo ICT per la protezione di canali di comunicazioni basati sul protocollo http. TLS va di fatto ad aggiungersi al protocollo http occupandosi in particolare della sicurezza della comunicazione.
In particolare, grazie a TLS è possibile stabilire comunicazioni:

- Private, non intelligibili quindi da sistemi diversi da quello origine e quello destinatario, grazie all’impiego di chiavi crittografiche simmetriche condivise tra i due attori al momento dell’iniziale processo di handshake.
- Autenticate, mediante tecniche di cifratura a chiave pubblica (PKI) che prevedono l’impiego di certificati digitali. Questa soluzione impiega la medesima tecnologia di certificati presente sul sistema TS/CNS.
- Affidabili, grazie ai meccanismi di verifica di integrità inclusi nel protocollo

Criptazione delle informazioni persistite

Non essendo il sistema Aggregatore dotato di una propria base dati permanente, il meccanismo di criptazione delle informazioni persistite si applica ai dati di configurazione, caching, audit e monitoraggio del sistema.
In particolare, la soluzione impiegata è la criptazione del file system Linux mediante:

- dm-crypt (driver)
- cryptsetup (tool utente per la predisposizione del FS)
- luks (gestore delle chiavi)

I dati vengono crittografati nella memoria permanente, se un disco rigido è fisicamente rimosso e installato su un'altra macchina è ancora completamente crittografato e può essere decodificato solo con la chiave appropriata.
Questa soluzione soddisfa il requisito di crittografia dei file in chiaro.

Configurazione sicura dell’infrastruttura

L’architettura applicativa del sistema impiega un modello multitier a tre livelli distinti:

- livello di presentazione od interfaccia utente: per la rappresentazione dei dati verso l’utente e della raccolta e verifica dei dati in ingresso;
- livello business logic o applicazione: per l’implementazione della logica di elaborazione dei dati; acquisisce i dati dal livello presentazione e dal livello data access, esegue elaborazioni su di essi e li restituisce elaborati ai livelli di presentazione e data access;
- livello data access: per l’accesso alle basi dati, per esempio basi dati permanenti/persistenti come database relazionali, ma anche servizi di accesso a dati dinamici.

Tale architettura multitier è configurata per esse sfruttata al massimo in termini di sicurezza:

- Tre sottoreti diverse, protette da firewall e con il traffico opportunamente filtrato in modo da garantire un accesso corretto a utenti con diritti diversi.
- L’accesso è consentito solo fra strati concomitanti: solo lo strato di business logic accede allo strato di persistenza; lo strato di presentazione accede solo allo strato di business logic. Non esiste interazione fra lo stato di presentazione e lo stato di persistenza.

L’architettura multitier è di per sé garanzia di un accesso “sicuro” ai dati, dato che lo strato di persistenza non deve mai essere esposto all’accesso diretto da parte dello strato di presentazione: la fruizione è filtrata dallo strato di business logic, a fronte delle quali è possibile accedere solo a determinate funzioni della logica applicativa.
Altro elemento di sicurezza intrinseca è la possibilità di intervenire su uno strato indipendentemente dagli altri, per evoluzione, distribuzione di una nuova versione, manutenzione.
Il sistema segue questo approccio di separazione dei livelli per garantire compartimentazione, separazione di privilegi, e modularità del software.

Tracciatura, analisi e notifiche delle attività di accesso

Il modulo di Audit e Analisi offre una componente per la gestione, l’analisi e la consultazione tramite interfaccia utente dedicata delle informazioni di Audit. L’accesso alle funzionalità e alla UI dedicata è regolamentato da opportuni controlli, al fine di proteggere adeguatamente le informazioni sensibili contenute.
Il modulo rientra nella categoria di software SIEM (Security Information and Event Management) ma, a differenza delle altre soluzioni di mercato, viene realizzata come soluzione verticale per il dominio sanitario della Regione ed è compatibile con i protocolli standard tipici sanitari quali IHE ATNA e HL7 FHIR (risorsa AuditEvent).
Le principali funzionalità e caratteristiche della soluzione applicativa Audit Analyzer sono riassunte di seguito:

- gestione centralizzata di audit trail/log applicativi prodotti dai software dipartimentali/verticali ad essa integrati
- integrità ed inalterabilità degli Audit, garantita mediate l’utilizzo di tecnologie basate su algoritmi di hashing
- meccanismi di analisi comportamentale proattiva degli Audit in ingresso (Data aggregation & correlation) che permette di effettuare analisi in tempo reale degli allarmi di sicurezza generati a partire dalla verifica dei messaggi di Audit creati e loggati dalle singole applicazioni
- possibilità di configurare la generazione e l’invio di allarmi, sulla base dell’analisi proattiva descritta precedentemente
- configurabilità del data retention, tempo entro il quale mantenere le informazioni di audit raccolte permettendo di definire diversi periodi di retention in funzione della tipologia di evento.

4. CONCLUSIONI

TBD

5. APPENDICE

5.1. RIFERIMENTI

Riferimento	Documento