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:

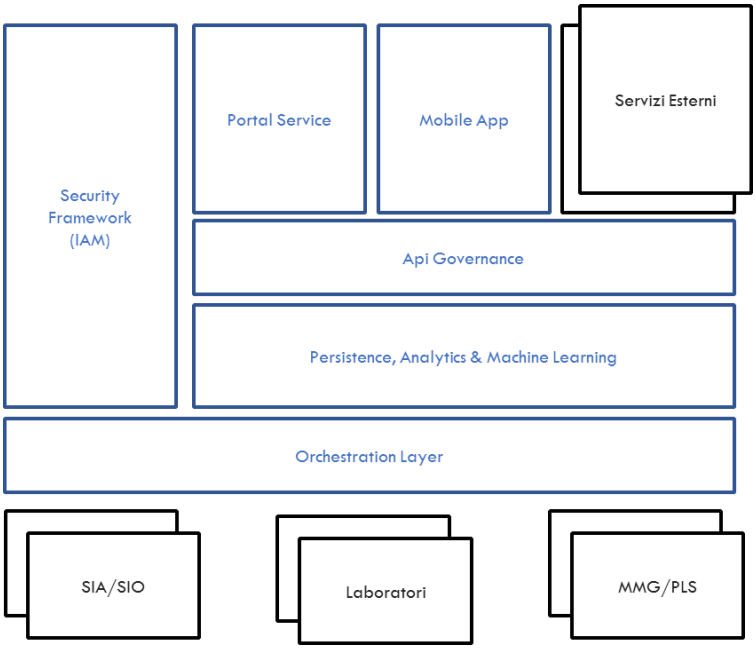

Figura 1 Architettura di alto livello della soluzione

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.

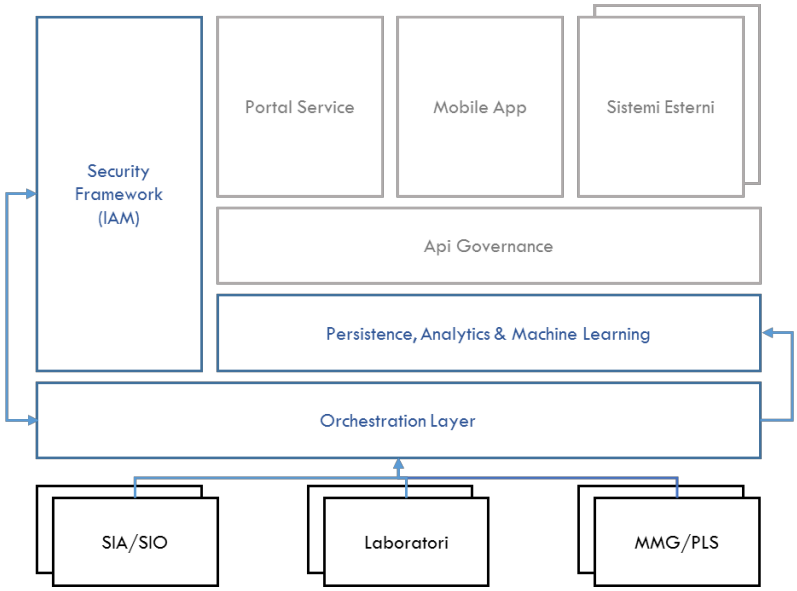

Figura 2 Ingestion dei Dati

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.

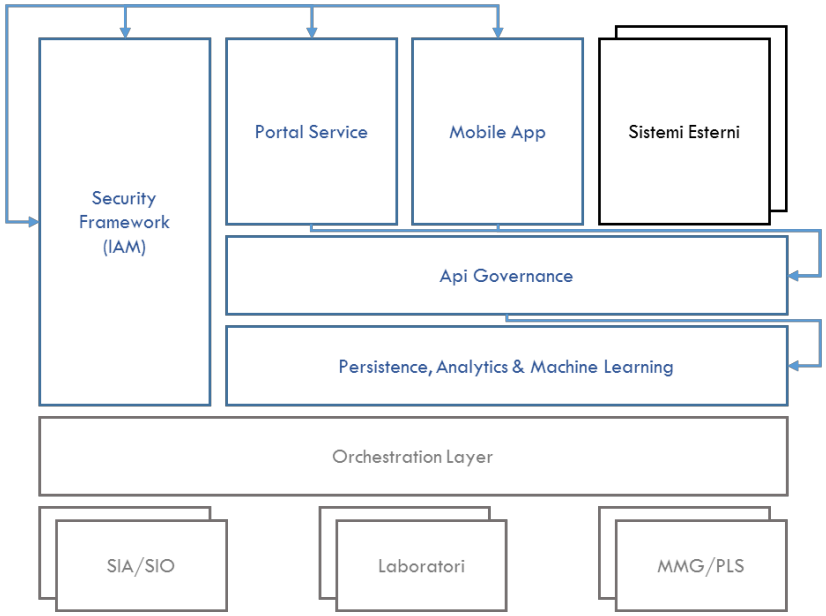

Figura 3 Service Layer

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:

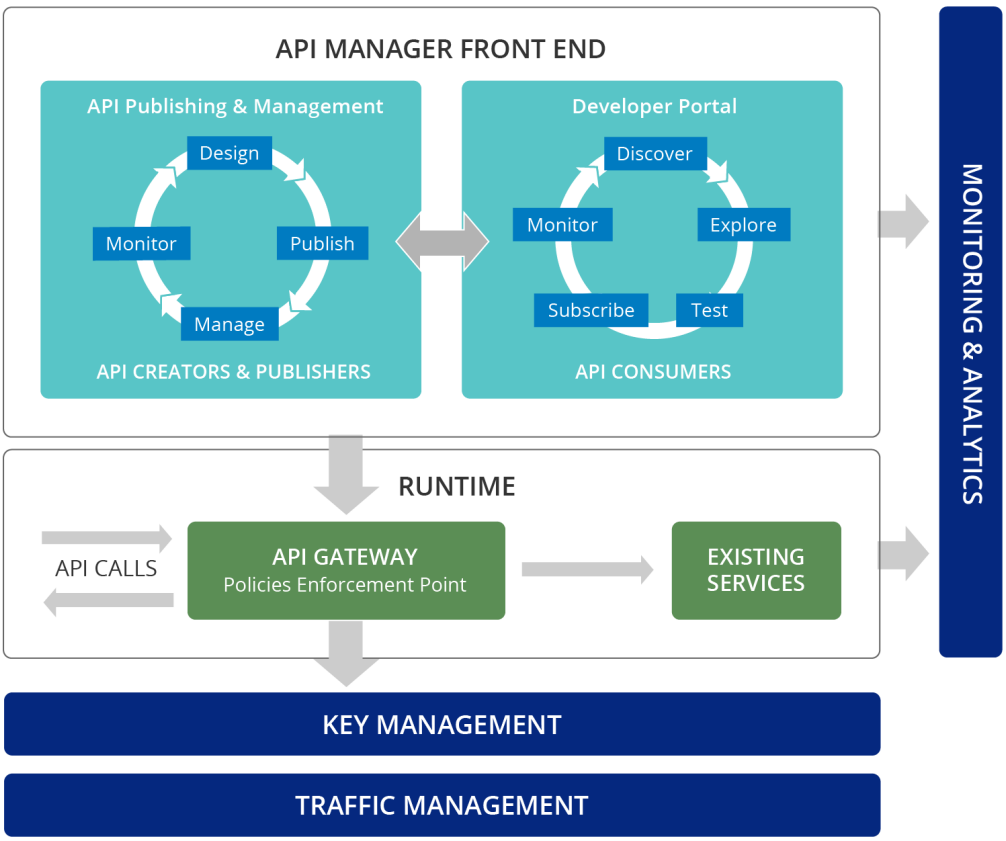

Figura 4 Api Manager

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.

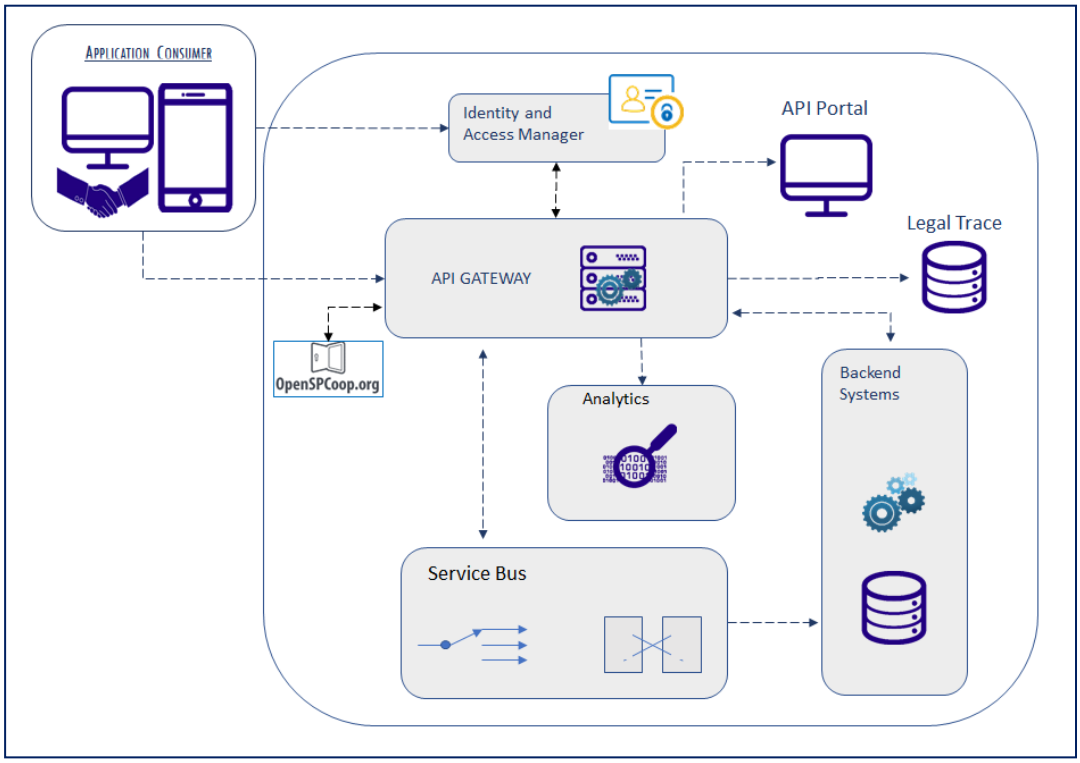

Figura 5 Api Gateway

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.

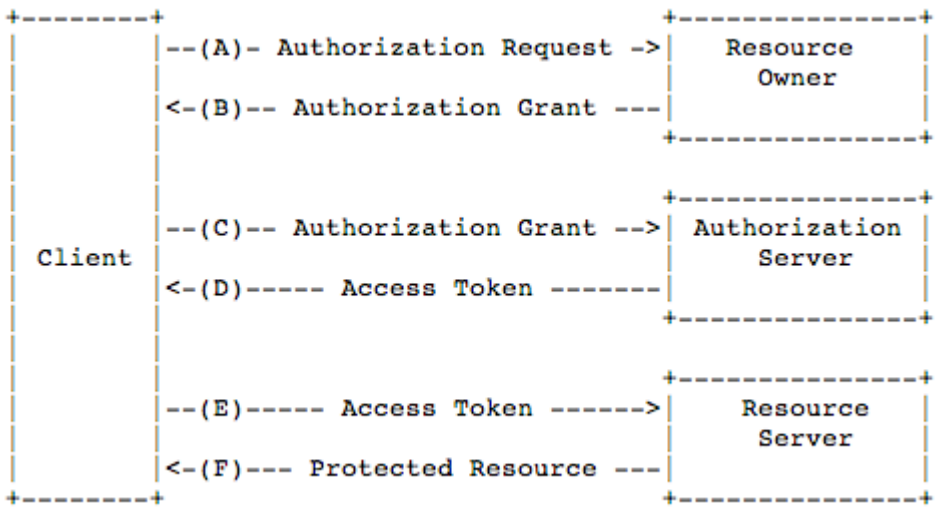

Figura 6- Flusso OAuth2

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.

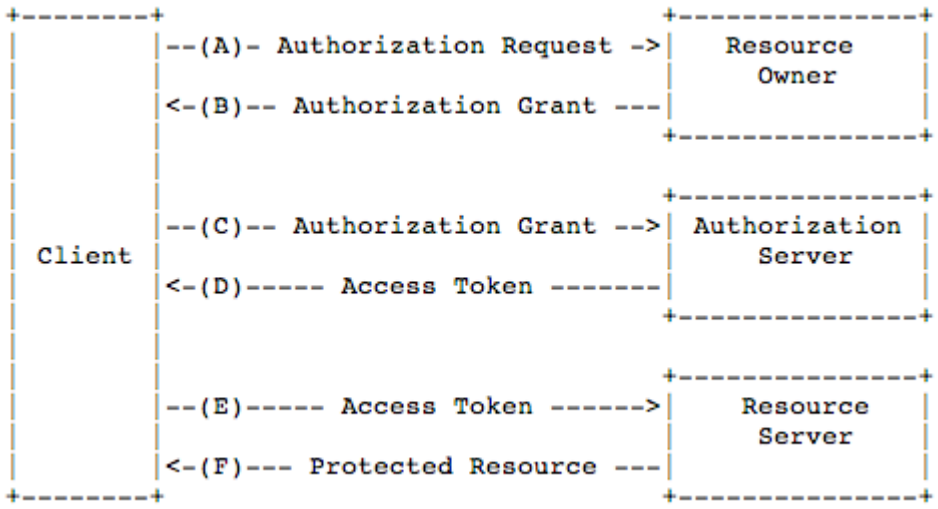

Figura 7 - OAuth2 Client Credentials

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.

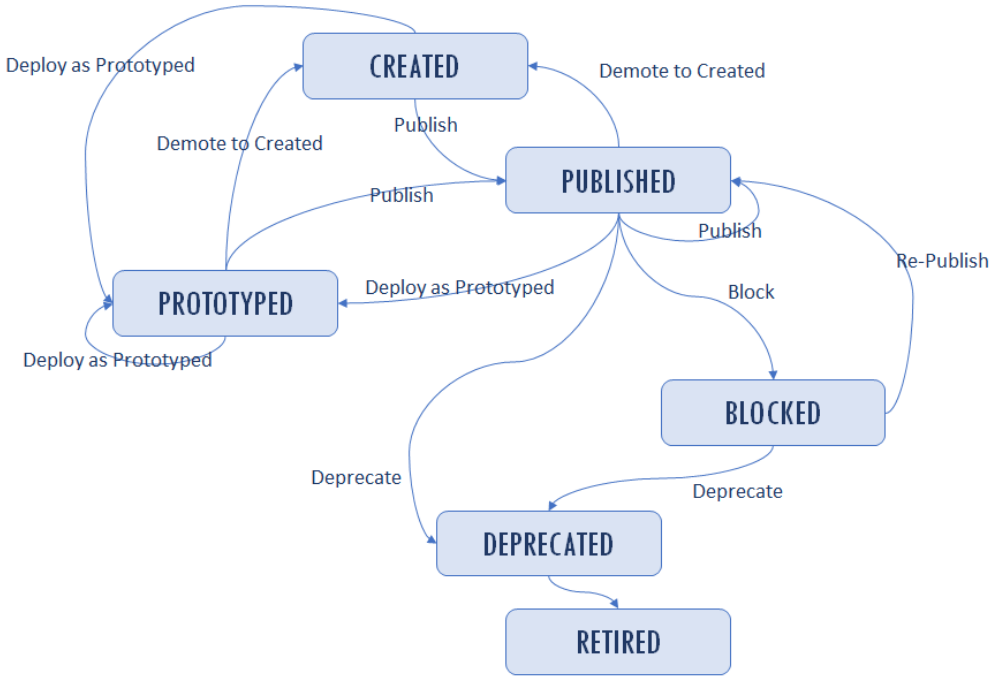

Figura 8 - Ciclo di vita dell'API

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:

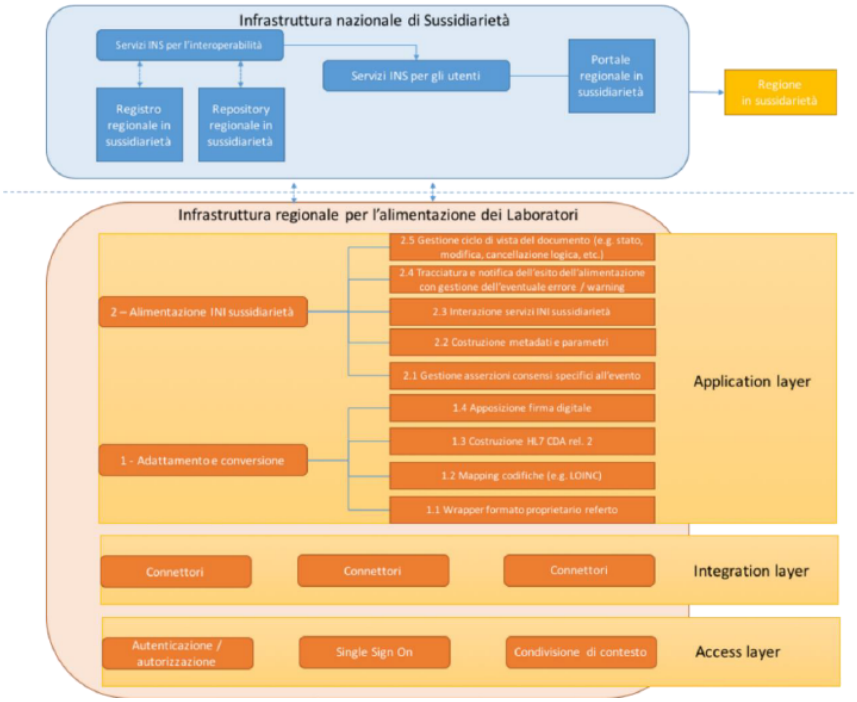

Figura 9 Vista funzionale

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:

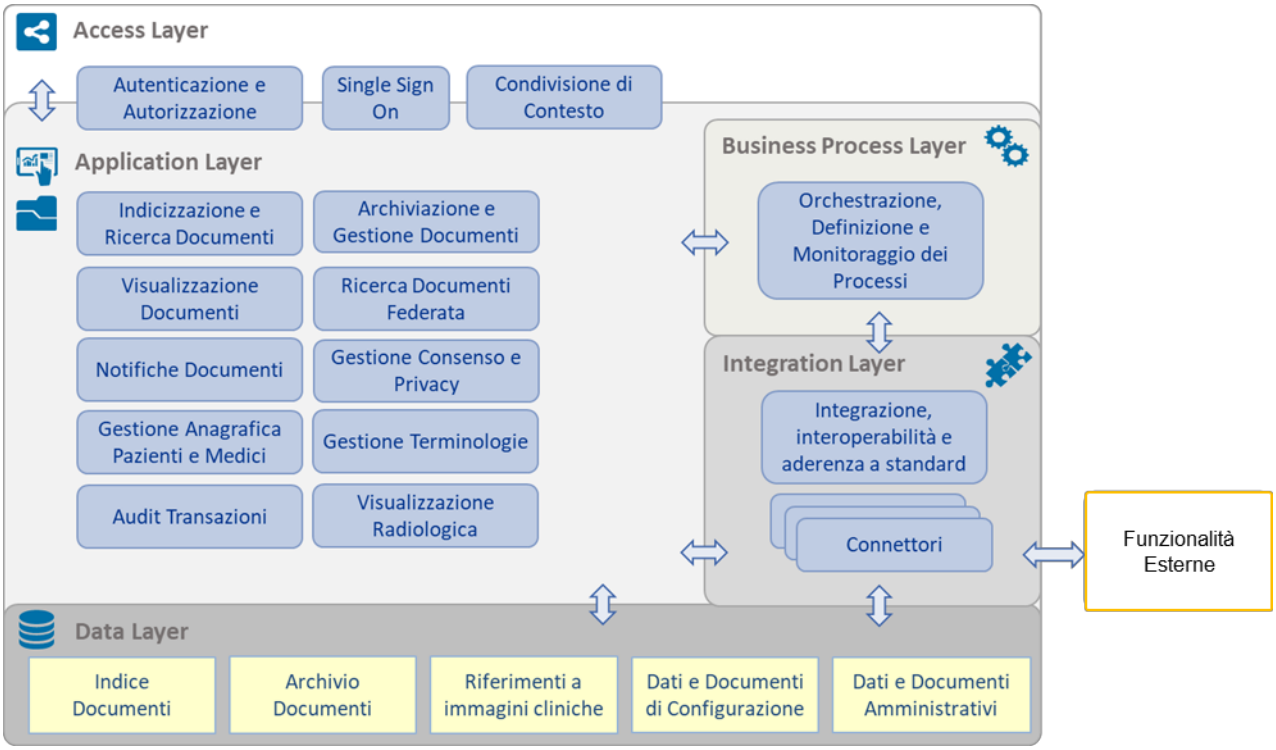

Figura 10 Architettura Funzionale

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